



Final Report

Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense

Information Assurance and Information Technology
Human Resources
Integrated Process Team

August 27, 1999

Office of the Secretary of Defense

Abstract and Keywords

Abstract: The DoD's warfighting capability and the security of its information infrastructure are at great risk from attacks by foreign intelligence organizations, cyber-terrorists, and the incompetencies of some of its own users. Just as dangerous is the shortage of adequately trained and managed information technology professionals, particularly in the area of information assurance. The shortage of trained people is also critical in other parts of the public sector and in the private sector as well. In 1998, the Deputy Secretary of Defense tasked Assistant Secretary of Defense (C3I) and the Under Secretary of Defense (P&R) to establish an Information Technology and Information Assurance Human Resources Integrated Process Team. This team would recommend actions, processes, and policies that would address the weakest link in DoD's defense of its information infrastructure—the people who use, administer, and manage it. The team, composed of representatives from 15 DoD organizations, concentrated on problems and issues in (1) workforce management and (2) IT and IA training and certification. In less than six months, the team developed a set of recommendations, projected results if the recommendations were implemented, cost estimates, and a five-year time line.

Keywords: Information technology (IT), information assurance (IA), Clinger-Cohen Competencies, workforce, manpower, human resources, management, weapons systems, computers, computer networks, Department of Defense, information security (INFOSEC), computer security, policies and procedures.

Contents

Executive Summary.....	ES-1
1. The Problems	1
1.1 Background.....	1
1.2 Goals of the IT/IA Human Resources Integrated Process Team.....	1
1.3 Overview of Problems and Issues	2
1.4 Data Collection and Analysis.....	4
2. Workforce Management	9
2.1 Findings and Recommendations.....	9
2.2 Discussion and Analysis.....	10
3. Training and Certification.....	13
3.1 IT Management Training: Findings and Recommendations.....	13
3.2 IT Management Training: Discussion and Analysis.....	13
3.3 IA Training: Findings and Conclusions	16
3.4 IA Training: Discussion and Analysis	17
4. Roadmap to Improvements	23
4.1 Implementing the IPT Recommendations.....	23
4.2 Priorities.....	24
4.3 Costs.....	25
4.4 Timeline for Implementation	25
4.5 Future Issues to be Addressed by OSD.....	25
Appendix A. Private Sector Recruiting and Retention Techniques	A-1
Appendix B. Recruiting and Retaining Information Technology Professionals.....	B-1
Appendix C. Clinger-Cohen Competencies (IT Functions)	C-1
Appendix D. Information Assurance Functions.....	D-1
Appendix E. Data Call Results.....	E-1
Appendix F. Military IT Occupational Specialties.....	F-1
Appendix G. Requirements for IT/IA Coding of DoD Manpower/Personnel Databases.....	G-1
Appendix H. Certification Requirements for System/Network Administrators.....	H-1

Appendix I. Certification Requirements for Threat and Vulnerability Assessments.....	I-1
Appendix J. Certification Requirements for Computer Emergency Response Team.....	J-1
Appendix K. Service/Agency Costs to Implement Recommendation	K-1
Appendix L. Schedule of Recommendations.....	L-1
References.....	Refs-1
Acronyms and Abbreviations.....	Acros-1

Figures

Figure 1.	Total Service Population Divided by Type of Major Command	E-4
Figure 2.	Framework for IA Results.....	E-5
Figure 3.	Summary of Service Infrastructure in IA Sampling Requirements	E-5
Figure 4.	IA Resource Distribution by Function for the Services	E-11
Figure 5.	Relative Distribution of DIA IA Resource by Function	E-13
Figure 6.	Relative Distribution of NIMA IA Resources by Function.....	E-13
Figure 7.	Reported DISA IA Resources by Function.....	E-14
Figure 8.	Personnel vs. Time Spent on IA for the Services.....	E-15
Figure 9.	Full-Time vs. Part-Time Distribution for DIA, DISA, JCS, and DLA	E-16
Figure 10.	Level of Training for the Services	E-17
Figure 11.	Personnel Background Breakdown for Army and Air Force.....	E-19
Figure 12.	Personnel Background for Selected DoD Agencies.....	E-19

Tables

Table ES- 1.	Recommendations and Their Priorities.....	ES-3
Table 1.	IPT Organization.....	2
Table 2.	Incentives – FY1997 Through March 1999	12
Table 3.	Anticipated Results and Implementation Status.....	23
Table 4.	IPT Recommendations and Their Costs.....	26
Table 5.	IA Functions.....	E-2
Table 6.	Sampling Plan for IA Data Call.....	E-6
Table 7.	IT Occupational Codes Within DoD	E-6
Table 8.	Data Call Response Received.....	E-8
Table 9.	Population Count Used to Scale the Services.....	E-10
Table 10.	Summary of IA Service Resources.....	E-12
Table 11.	Level of Training for the Agencies.....	E-18
Table 12.	Information Management (3A)	F-5
Table 13.	Communications/Computer Systems Operator (3C).....	F-5
Table 14.	Computer-Computer Systems Operations (3C0X1).....	F-6
Table 15.	Computer-Computer Systems Programming (3C0X2).....	F-6
Table 16.	Radio Communications Systems (3C1X1)	F-6
Table 17.	Electronics Spectrum Management (3C1X2).....	F-7
Table 18.	Computer-Computer Systems Control (3C2X1).....	F-7
Table 19.	Planning and Implementation (3C3X1).....	F-7
Table 20.	Communications and Information Officer (33S).....	F-8
Table 21.	Communications and Information Systems (33SX).....	F-8

Table 22.	Communications/Computer Systems Engineer (33XSA).....	F-9
Table 23.	Information Systems Operator Analyst (74B).....	F-10
Table 24.	Telecommunications Operator-Maintainer (74C).....	F-10
Table 25.	Telecommunications Computer Operator- Maintainer (74G)	F-10
Table 26.	Information Systems Chief (74Z)	F-11
Table 27.	Information Systems Management (AOC 53A).....	F-11
Table 28.	Signal (Information Systems) Operations (AOC 25A)	F-12
Table 29.	Network Management Technician (MOS 250N).....	F-12
Table 30.	Automation Technician (MOS 251A).....	F-13
Table 31.	Radioman.....	F-14
Table 32.	Information Systems Administrator (NEC 2735).....	F-14
Table 33.	Network Security Vulnerability Technician (NEC2780)	F-15
Table 34.	Information Systems Security Manager (NEC 2779).....	F-15
Table 35.	Advanced Network Analyst (NEC 2781).....	F-15
Table 36.	Navy Officer IT Subspecialties.....	F-16
Table 37.	Navy Officer Subspecialties – Billets vs. Inventory	F-17
Table 38.	Small Computer Systems Specialist (MOS 4066)	F-18
Table 39.	Communications Information Systems Officer (MOS 0602).....	F-19
Table 40.	Certification Requirements of System/Network Administration & Operations.....	H-2
Table 41.	Certification Requirements for Threat & Vulnerability Assessment.....	I-2
Table 42.	Certification Requirements for CERT.....	J-2
Table 43.	Service/Agency Costs to Implement Recommendations.....	K-1

Definitions and Conventions Used in This Report

Although normally definitions are placed in an appendix, there are five terms used throughout this report that *must* be understood for accurate comprehension. For this reason, they are defined in the front of the report.

Term	Definition	For More Information
IT Workforce	Includes all people, military, civilian, and contractor, in the Department who perform functions identified in the Clinger-Cohen Competencies regardless of their occupational specialties.	Clinger-Cohen Competencies listed in Appendix C.
IT Professional	A subset of the IT workforce—includes only those people, military, civilian, and contractor, in the Department who perform functions identified in the Clinger-Cohen Competencies and whose primary occupational specialty is defined as an IT occupational specialty.	Clinger-Cohen Competencies listed in Appendix C.
IA Workforce	Includes all people, military, civilian, and contractor, in the Department who perform IA functions regardless of their occupational specialties.	IA functions listed in Appendix D.
IA Professional	A subset of the IA workforce—includes only those people, military, civilian, and contractor, in the Department who perform IA functions and whose primary occupational specialty is defined as an IT occupational specialty.	IA functions listed in Appendix D.
Privileged Access	A special access above those privileges required for the normal data acquisition or operation of an information system. This access grants capabilities to a user, operator, administrator, maintainer, auditor, or any other person that enable them to alter or affect the intended behavior or proper content of a system, as well as alter or affect the capabilities or data of any other user of the information system.	

Executive Summary

Purpose

This report presents the findings and recommendations of the Information Assurance (IA) and Information Technology (IT) Human Resources Integrated Process Team (IPT). The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and the Under Secretary of Defense (Personnel and Readiness) jointly commissioned the IPT in September 1998. They charged it to identify the critical IA and IT Management skill sets in the Department of Defense (DoD) and to recommend mechanisms that would promote the achievement and sustainability of those skills in the Department.

Forty-five people from fifteen DoD Services and Agencies met for the first time in late September 1998 to begin an intensive six-month analysis of the above tasking. Their goal was to recommend actions and policies that would lead to establishing a comprehensive and world-class human resources program for IA and IT Management within the Department.

The IPT looked closely at the following areas

- Taxonomy
- Occupational descriptions and career fields
- Certification standards
- Training programs
- Accession and retention trends

Findings

Generally, there is no Department-wide recognition of the very real and growing threat to our warfighting capability as evidenced by inadequate priority, funding, training, and focus on information assurance.

The IPT's most significant finding was that IA and IT Management personnel readiness is more problematic than simply providing training opportunities and financial/career

incentives to IT professionals. Before those strategies can be attempted, the Department must learn the demographics of its IT population and know precisely what IT activities it is performing. Today, the Department is unable to expeditiously determine this information. The reasons are many, but the primary causes are that some people in non-IT career fields are performing ill-defined IA functions part time and that frequently civilian occupational series are not tied directly to IT functions. The report indicates that this fact makes it difficult to determine precisely who has access to the Department's information infrastructures. Furthermore, it makes it almost impossible to regulate training and certification requirements in what is basically a transient work force. Lastly, trying to enhance career opportunities among this unidentifiable work force is extremely difficult.

Recommendations

The IPT therefore recommends changes to the ways in which the Department manages its IT workforce. One change takes the form of recognizing specific IA functions that reflect current duties of the information age. Also, the IPT recommends coding IT billets and all people who perform IT functions in DoD personnel databases so that their career progression trends and training credits can be accurately tracked. Lastly, the IPT suggests tying standardized training and certification requirements to those coded billets and people so that no one with privileged access to information infrastructures is overlooked when it comes to critical IT preparatory and sustaining education.

In four chapters and twelve appendices, the IPT report presents a strong case that the Department should take preliminary steps that will substantially improve the way we manage our IA and IT workforce. The IPT concludes that in three to five years after these

recommendations are fully implemented, the Department will have the presently non-existent personnel data needed to make proper decisions concerning the creation of a career management program for IT personnel. Supporting this conclusion are nineteen distinct recommendations and associated cost estimates that—if enacted—will vastly improve the Department's IA and IT Management personnel posture.

These recommendations suggest that CINCs, Services, and Agencies adopt a consistent IA terminology and standardized Certification Criteria for certain IA functions. Recommendations further state that no one be allowed to perform these specified critical IA functions without benefit of prior training.

The recommendations also address the need for IT Management education and call for the creation of Advanced Distributed Learning programs. Equally important is the report identifies the DoD entities responsible for implementing each recommendation.

Finally, the report concludes with an implementation timeline that recognizes the major steps to complete the recommendations and the schedule for doing so. Although the timeline reflects five years for full implementation, the IPT believes that effective management and sufficient priority will result in substantive incremental progress each year, beginning with the first year.

The costs to implement these recommendations are significant in people, time, and money. If totally enacted, they will cost approximately \$77.5 million over the next five years. However, the IPT is confident that the suggested course is a prudent one to position the Department appropriately in the Information Age.

The risks to our information resources are well known and the strengths of our information infrastructure defenses are being tested daily. *The weakest link in those defenses is not the technology but the people who use, administer, and manage it.* Ensuring that those people are adequately prepared for the challenge is the ultimate benefit of the IPT's work.

Table ES- 1. Recommendations and Their Priorities

Priority 1: Recommendations that have a direct impact on substantially improving the Department's ability to protect the integrity and availability of its information systems and networks and its ability to operate effectively in a joint warfighting environment.

Priority 2: Recommendations that enable the Department to substantially improve its ability to manage its IT workforce or which provide long-term efficiencies for Priority 1 recommendations.

Priority 3: Recommendations that enable the Department to improve the quality of its IT workforce and maintain improvements realized as a result of implementing Priority 1 recommendations.

Priority 4: Recommendations that will provide official policy guidance to support the recommendations above.

If the DoD Implements...	The Results Would Be...	Implementation Status
Recommendation 1: Direct the OUSD (P&R) to establish the requirement that the CINCs, Services, and Agencies identify manpower and personnel assigned IT/IA functions, enter the required information into the appropriate databases, and maintain these databases as changes occur. (Priority 2)	The Department's IT and IA workforces, both authorized billets and positions and personnel, will be able to be systematically and continually identified and quantified. This capability will be institutionalized.	Implementation in the mode of "business-as-usual" will require about three years once funding is provided. If sufficient priority is given to this recommendation, completion could be realized in about 18 to 24 months.
Recommendation 2: Direct the OASD (C3I) to work with the OUSD (A&T) and the OUSD (P&R), as part of the Inherently Governmental Working Group (IGWG), to revise IT function codes and develop definitions that more accurately reflect today's IT and IA activities. (Priority 2) Recommendation 3: Direct the OASD (C3I) to draft guidance for review by the Inherently Governmental Working Group to be used by the DoD Components to determine core IT and IA requirements to minimize the risk of losing mission capability. (Priority 2) Recommendation 4: Direct the OUSD (A&T) to consider the merits of developing and maintaining a database that shows contractor staff-years against major functions, especially IT and IA. (Priority 4)	The Department will have more accurate information about its government and contractor mix in the IT/IA workforce. A mechanism will be in place to maintain a core capability in these critical functions and to assess the risk of additional outsourcing.	Work is being currently initiated in these areas. By next year, information will be available to begin examination of outsourcing issues and risks.
Recommendation 5: Direct the ODASD (MPP) to establish a steering group comprised of OSD, Joint Staff, and each of the Services (including the Coast Guard) to focus on military IT personnel issues. (Priority 3)	The Department will have a forum for Services' military IT career managers to identify and assess improved methods for managing their people.	Implementation could be completed within three months or less and continue as long as the shortage of IT personnel is a serious problem.
Recommendation 6: Direct the ODASD (CPP) to work with the ASD (C3I) to widely publicize OPM flexibilities available to address civilian IT recruiting and retention problems. (Priority 2)	Local commanders and directors will have better information on already-approved civilian personnel management capabilities to improve their ability to recruit and retain civilian IT professionals.	Implementation can be completed within three months. The use of recruiting bonuses and retention allowances can be tracked on a regular basis.

If the DoD Implements...	The Results Would Be...	Implementation Status
<p>Recommendation 7: Direct the OASD (C3I) to require the staffs of the DoD CIOs at the GS-13 through the GS-15 levels to complete the DoD CIO Certificate Program or the Advanced Management Program at the IRMC. Components that wish to use ITM training programs other than IRMC will submit verification of equivalency to the DCIO office to ensure training programs cover mandatory requirements of the Clinger-Cohen Act and the Department's implementation strategies. (Priority 3)</p> <p>Recommendation 8: Direct the OUSD (P&R) and the OASD (C3I) to issue policy directing the Services/Agencies to implement a mandatory requirement that DoD CIOs, Deputy CIOs, and SESs and flag officers on the CIO staffs attend DoD-sponsored ITM executive sessions. (Priority 3)</p> <p>Recommendation 9: Direct the OUSD (Comptroller) to provide resources (personnel and funding) to the IRMC to accommodate additional training requirements of the DoD ITM workforce. (Priority 3)</p> <p>Recommendation 10: Direct the OASD (C3I) to work with the Joint Staff and the ODASD (CPP) to develop an IT contemporary issues training module for the CAPSTONE and APEX training sessions. (Priority 2)</p>	<p>IT training for the Department's senior executives (military and civilians) and CIO staffs will meet the requirements of the Clinger-Cohen Act.</p>	<p>CIO staff training can begin immediately. However, funding is necessary to accommodate additional throughput of students and the development of course and curricula to address new IT training requirements.</p>
<p>Recommendation 11: Direct the OASD (C3I) to officially adopt NSTISSI Number 4009, <i>National Information Systems Security (INFOSEC) Glossary</i>, as the official IA Glossary. This requires the Defense-wide Information Assurance Program (DIAP) to formally coordinate an annex defining terminology not yet officially adopted by NSTISSI but used by the Department. (Priority 4)</p> <p>Recommendation 12: Direct the Joint Staff to review the defensive information operations requirements in the context of JV 2010 and translate these requirements into the Universal Joint Task List (UJTL) and the Joint Mission Essential Task List (JMETL). (Priority 4)</p> <p>Recommendation 13: Direct the OASD (C3I) to officially adopt the NIST Special Publication 800-16, <i>Information Technology Security Training Requirements: A Role- and Performance-Based Model</i> and the NSTISSIs as the minimum DoD IA training standards. (Priority 4)</p>	<p>The Department will have a common IA language, a common reference point for joint training requirements, and a baseline IA training standard.</p>	<p>Adoption of the NSTISSI Glossary and training standards can be implemented within three months. Development of a DoD Glossary supplement and UJTL and JMETL modifications can be implemented within six months.</p>

If the DoD Implements...	The Results Would Be...	Implementation Status
<p>Recommendation 14: Direct the OUSD (P&R) and the OASD (C3I) to establish the requirement that the CINCs, Services, and Agencies establish mandatory training and/or certification programs for the five “critical” IA functions, using the NSTISSC training standards and the IPT-developed certification requirements as the minimum requirement. In support of this, DISA shall develop baseline IA training courses to meet the IA training requirements stipulated in the IPT certification documents. These courses can then be used by the Services and Agencies to meet the certification IA training requirement or enhanced by the Service and Agency to meet its unique needs. (Priority 1)</p> <p>Recommendation 15: Direct the OASD (C3I) to establish the requirement that no person assigned to a “critical” IA function at the entry level may be granted privileged access until the required IA training is successfully completed. (Priority 1)</p> <p>Recommendation 17: Direct the OUSD (P&R) and the OASD (C3I), in concert with the CINCs, Services, and Agencies, to coordinate biennial reviews of each certification and/or training program to ensure the currency and utility of the requirements. (Priority 3)</p>	<p>The Department will have increased assurance about the reliability of the IA workforce and its ability to protect the integrity and availability of the Department’s interoperable and networked information systems. An institutionalized certification process will replace today’s non-existent standards, including maintaining the currency of the standards.</p>	<p>Although full implementation will require three to five years once funding is provided, substantial progress can be achieved annually if appropriate priority is given to the effort.</p>
<p>Recommendation 16: Direct the OUSD (P&R) and the OASD (C3I) to establish the requirement that the CINCs, Services, and Agencies document these certification programs in full and develop the capability to readily produce detailed answers about the status of certifications. (Priority 3)</p> <p>Recommendation 18: Direct the OUSD (P&R) and the OASD (C3I) to develop and establish an Advanced Distributed Learning program, including a certification management system, for IA training and education at DISA or other appropriate location. The IA Advanced Distributed Learning effort will support implementation of an IA element within the Federal Center for Information Technology Excellence proposed under PDD 63. (Priority 2)</p>	<p>The Department will have the capability to maintain current IA training modules and deliver this training to the workforce in a timely and cost-effective manner as well as track the currency of the workforce’s certification.</p>	<p>Although it will take five years to fully implement these recommendations, by capitalizing on similar work already completed, the requirements can be prioritized, with specific capabilities completed progressively beginning with the first year after funding is provided.</p>
<p>Recommendation 19: Direct the OASD (C3I) to incorporate into the DODIR 8500.xx, <i>Information Assurance</i>, the requirement for contractors assigned “critical” IA functions to meet the same or equivalent certification and training requirements as Department personnel. This recommendation requires that the OUSD (A&T) provide guidance to Contracting Officers to ensure these requirements are included in affected contracts. (Priority 1)</p>	<p>The Department’s IT/IA contractors will meet the same minimum training and certification requirements as our military personnel and civilian employees.</p>	<p>The policy can be promulgated within six months. All new contracts would meet the requirements from the time the policy was promulgated. Estimates are up to two years before all existing contracts requiring changes are amended.</p>

1. The Problems

1.1 Background

There is a growing shortage of information technology (IT) professionals worldwide. This has caused major competition between the private and public sectors in hiring and maintaining skilled IT personnel to meet the rapidly expanding technological needs of organizations. Coupled with this, there is also a growing concern regarding information security. The Department of Defense (DoD) is an information- and technology-dependent organization. Mission accomplishment, including the ability to maintain a secure information infrastructure, is at great risk if the required IT professionals are not available.

In May 1996, the General Accounting Office (GAO) published its report, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. This GAO report provided an excellent summary of the growing threat to the information infrastructure of the DoD. Additional support for this situation was provided in the November 1996 Defense Science Board (DSB) *Report on Information Warfare – Defense*.

If the findings of both the GAO and DSB reports are viewed in the context of Joint Vision (JV) 2010, the prognosis for achieving the JV 2010 goal of information superiority is bleak. Recent events and exercises such as Solar Sunrise, Eligible Receiver, and Evident Surprise confirm these findings. Further, since the GAO publication, the DoD continues to sustain specific documented attacks to its information infrastructure, again adding credence to the report's findings: *The Department's warfighting capability and the security of its supporting information infrastructure are at great risk*. Fixing the problem requires commitment at all levels of management and leadership to:

- Ensure complete understanding, throughout the Department, of the issues and attendant risks to mission accomplishment.
- Revise and establish policies that reflect the information technology environment of today and tomorrow.
- Mandate minimum standards and continuous risk assessment for the protection, integrity, and availability of the Department's information infrastructure.
- Provide resources, both dollars and people, to maintain an acceptable level of risk in protecting the integrity and availability of DoD information systems.

1.2 Goals of the IT/IA Human Resources Integrated Process Team

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD (C3I)) and the Under Secretary of Defense (Personnel and Readiness) (USD (P&R)), responding to tasking from the Deputy Secretary of Defense (DEPSECDEF), established an Information Technology (IT)/Information Assurance (IA) Human Resources Integrated

Process Team (IPT) on September 22, 1998, to address the human resources issues raised in the GAO report as well as in subsequent reports by the DoD Inspector General (DoDIG), DSB, and internal studies on the Department's information infrastructure. The goals of the IPT were to recommend actions and policies that would:

- Identify critical IA and information technology management (ITM) knowledge and skills.
- Create mechanism(s) to assess and certify individual competencies.
- Establish well-defined occupational descriptions and career fields.
- Monitor accession and retention trends.
- Develop and implement training programs.
- Identify barriers to implementation.

The IPT was established under the Office of the Secretary of Defense (OSD) leadership of:

- Kenneth Scheflen, Director, Defense Manpower Data Center;
- Richard Schaeffer, Director, Information Assurance; and
- Kim Corthell, Director, Information Policy.

The IPT was organized into three subgroups with membership from the Services and Agencies as shown in Table 1.

Table 1. IPT Organization

Information Assurance	Information Technology Management	Personnel Policy
Membership		
DIA	Marine Corps	DLA
NSA	OSD (P&R) (C3I)	WHS
Army	(IG) (A&T)	NIMA
Navy	Joint Staff	BMDO
Air Force	DFAS	
DISA	DSS	

OSD originally allotted the IPT 120 days to complete its work. However, given the complexity of the assignment and the Department's inability to readily provide the team with needed foundation data about existing IT and IA human resources, the IPT required an extra 60 days.

1.3 Overview of Problems and Issues

The current problems in the Department's IT and IA human resources management must be understood in the dynamically changing technological, economic, and environmental context. It is clear that our IT/IA human resources management increasingly lagged behind

the rapid expansion of and technological growth in information systems, especially with respect to the Department's overwhelming dependence on information technology. The IPT focused on problems and issues in (1) workforce management and (2) IT and IA training and certification. These are briefly described in the next sections.

1.3.1 Workforce Management

The promise of streamlined operations and improved efficiency often resulted in projected personnel savings being taken simultaneously with the technology procurements during the budget process. At the outset of the information technology revolution, Service commanders and Agency leaders used their local budget authority to purchase additional systems without understanding the human resource implications. They routinely decreased their human resource requirements to justify their technical procurements, basing these decreases on the promise of streamlined operations and improved efficiency resulting from the new technologies. Although the information systems acquisition process is much better understood and managed today, the Agencies and Services have not been able to address the resulting human resource shortages to manage and protect our existing information systems. In an effort to address this shortfall, leaders across the DoD, have relied on the self-taught computer "hobbyist" to fill the gap.

The Office of Personnel Management (OPM) authorized specific flexibilities for civilian personnel to help address the government-wide recruiting and retention problems facing managers. Few of these flexibilities are being used within the Department. Further exacerbating the IT workforce problems are DoD initiatives such as the recent major downsizing of our military and civilian workforces and the increased emphasis on outsourcing. Such initiatives tend to mask the supply problem in the Department.

When the situation is viewed in a broader context, the complexities of solving the problem are evident. Shortages in the supply of IT professionals are not confined to the DoD—they exist for other federal agencies and nationally in the private sector. Recruiting is difficult when colleges and universities are only producing enough IT graduates to fill half of the growing annual requirement. Several U.S. companies have begun recruiting foreign nationals to fill their IT jobs. Under the H-1B non-immigrant category of U.S. immigration law, U.S. employers may sponsor 65,000 professional foreign nationals each year. These workers must have a professional undergraduate degree or substantial work experience and may work in the United States for six years. This was just one congressional effort to try to narrow the gap. The turnover rate among IT professionals in the private sector is 30%, five times the rate for the private sector as a whole. Interviews with thirteen DoD IT contractors provided information on private sector IT recruiting and retention techniques. See Appendix A of a summary list of "best practices" in the private sector to combat the very real recruiting and retention issues.

The Department's ability to compete with the private sector in the area of compensation is limited by personnel practices and guidelines. It is also limited by law in the case of military personnel. The private sector can react quickly to any substantive compensation change made in the government. However, more extensive use should be made of the document issued by OPM, *Recruiting and Retaining Information Technology Professionals*, to acquire and maintain a stable civilian workforce of IT professionals within the Department. See

Appendix B for a copy of this OPM report. To acquire and maintain military IT professionals, the Services are currently using and expanding the use of enlistment and reenlistment incentives and bonuses for enlisted personnel.

1.3.2 IT and IA Training and Certification

The level and content of training in the Department varies. In some areas there are comprehensive training programs available for all DoD personnel such as the DoD Chief Information Office-sponsored programs at the National Defense University (NDU). Unfortunately, the Department does not take full advantage of these programs. In other cases, such as information assurance, training has been either unavailable or too expensive for some of the IA workforce. As a result, the level of training for our IT/IA workforce is uneven at best. The training content varies across the Department. This is a potentially serious threat to the Department's joint warfighting capability. Aside from those Agencies with technical missions, there are few career management programs (with management being the operative word) for the Department's civilian IT professionals.

1.4 Data Collection and Analysis.

The IPT's early attempts to identify and quantify Department personnel assigned IT and IA functions ran into a number of significant—and enduring—barriers. The IPT's experiences warranted a separate section documenting the problems as they pertain to collecting data on the subject of this report. We start first with discussing briefly the standard approach to evaluating workforce management, our efforts at evaluating, and then the modifications and “work-arounds” necessary to obtain, at the minimum, qualitative data and anecdotal evidence.

1.4.1 The Approach

The generally accepted methodology used to evaluate workforce management is to (1) define the functions performed by the workforce; (2) identify the requirements, authorized billets and positions, and personnel assigned those functions; (3) analyze the career structure and personnel issues such as accessions, retention, relative compensation (including benefits), career growth potential; (4) evaluate the effectiveness of the career management programs; and (5) recommend improvements.

In defining the functions performed by DoD IT/IA executives and personnel, the IPT used the Federally adopted Clinger-Cohen Competencies (listed in Appendix C) to define the functions of the IT workforce as a whole. The IA functions, although in existence, had not been codified or defined; therefore, the IPT identified a set of eleven functions (listed in Appendix D) that encompass all the IA functions currently performed in the Department. From the list of eleven functions, the IPT further defined five of these functions as “critical,” requiring privileged access. Privileged access is defined to be a special access above those privileges required for the normal data acquisition or operation of an information system. This access grants capabilities to a user, operator, administrator, maintainer, auditor, or any other person that would enable them to alter or affect the

intended behavior or proper content of a system as well as the capabilities or data of any other user of the information system. *The first step of the IPT study was accomplished.*

1.4.2 Personnel Classification Systems

The next step was to identify requirements, authorized billets and positions, and personnel assigned to IT/IA functions. The DoD personnel classification systems and personnel assignment systems contributed to the IPT's difficulty in clearly defining the IT workforce.

- (1) The military Services have specific military IT occupational specialties which have undergone intensive Service review and restructuring in the past three years. Personnel in these IT occupational specialties are managed as IT professionals. Accessions, retention, career development and progression, job assignments, and education and training are all major components of the centralized Service management of these 50,000 IT professionals. The management of this workforce is further discussed in Section 2.2.1.
- (2) The military Services assign other military personnel who are not in specific military IT occupational specialties to IT functions. Possible reasons for this situation include:
 - There are insufficient authorized IT billets and therefore insufficient IT personnel.
 - There are authorized IT billets but insufficient IT personnel to fill these billets.
 - Non-IT occupational specialties (e.g., finance, base supply, medical, maintenance) where the non-IT functional expertise is required, but IT skills are also required.

Identifying and quantifying these people is not a current or planned capability of the military Services.

- (3) There are five civilian occupational series that few people would dispute as being IT occupational specialties:
 - GS-332 – Computer Operator
 - GS-334 – Computer Specialist
 - GS-335 – Computer Clerk/Assistant
 - GS-854 – Computer Engineer
 - GS-1550 – Computer Scientist

In March 1997, there were 34,000 people in these occupational specialties (not counting the National Security Agency (NSA), the Defense Intelligence Agency

(DIA), and the National Imaging and Mapping Agency (NIMA)). While there are centralized career programs for positions that can be categorized as IT positions, civilian assignments to these positions are not centrally managed as are military assignments. In certain functional areas including information management, the Military Departments manage some of their grade 12 and above civilians centrally. However, these programs do not encompass all of those involved in information technology and information assurance functions.

- (4) There are additional civilians who are considered to be IT professionals because of their training, education, job experience, and assigned functions. However, these people are in a variety of occupational series. Identifying and quantifying the IT professionals in these series is not a current or planned capability of the Services or Agencies.
- There are insufficient authorized IT positions and therefore insufficient IT personnel.
 - There are authorized IT positions but insufficient IT personnel to fill these positions.
 - There are additional civilians who would not be considered IT professionals (i.e., they do not fit into either of the above two categories) but are assigned IT functions.

This group is similar to item (2) for the military personnel.

Identifying and quantifying these people is not a current or planned capability of the Services or Agencies.

- (5) Finally, there are the contractors who perform IT functions as IT professionals for the Department under contract. The full-time equivalent staff-years in this category are unknown because there is no mechanism in place to collect contractor staff-years by function.

1.4.3 Personnel Management Systems

Military and civilian personnel in general terms are managed very differently.

- The military personnel system is essentially a closed system whereby people enter the Service at the entry level and are promoted, over time, to higher levels. The civilian personnel system is an open system, whereby people can enter at whatever level for which they qualify based on education and experience.
- Military personnel have little choice in job assignment and/or duty location. The needs of the Service dictate both of these. Civilian personnel can choose both specific jobs and duty location.
- The Services are given wide latitude in establishing occupational career fields. Civilians' occupational series are governed by those series established and defined by OPM.

It is not reasonable to expect the Services or Agencies to manage a workforce that cannot be identified or quantified. The 50,000 military IT professionals discussed in item (1) can be and are managed. The 34,000 civilian IT professionals addressed in item (3) are only a part of the civilian IT professional workforce. Without the ability to identify the civilians who are part of item (4), it is difficult to impossible to identify possible improvements to our management systems.

Analyzing management options for those military and civilian personnel addressed in items (2) and (5) requires knowledge of the identity and quantity of people in these categories. Otherwise, it is not possible to estimate the dollar or management impact of any proposed changes. Currently there is insufficient data available that would allow the Department to calculate what percentage of its IT workload is accomplished by contractors and what percentage is accomplished by our military personnel and civilian employees.

1.4.4 Data Call

For all of the reasons cited in the previous sections, we cannot quantify or document our Department's IT recruiting or retention problems. We cannot project training and education requirements or costs for the civilian IT professional workforce nor can we project costs for compensation proposals.

In an effort to learn more about the IT workforce, the IPT elected to focus on the IA functions since these functions—if not performed properly—directly affect the security of our infrastructure. To quantify the characteristics of the IA workforce, the IPT completed a data call among the Services and Agencies. The IPT's original intent was to:

- Size the IA workforce;
- Quantify what percentage of the IA workforce was in other than IT occupational specialties;
- Quantify what percentage of the IA workforce had no formal training;
- Identify the occupational specialties being used to perform IA functions; and
- Quantify the workforce size by IA function.

This data call process is described in detail in Appendix E. Although data collected through a data call reflects only a single point in time, the IPT did learn some important facts from the conduct of the data call and the analysis of the data.

- Collecting data at the unit level (bottom up) is a time-consuming and problematic process. It took approximately two months to get approval for the data call and, after an additional five months, the response rate was well under 25%, making it difficult to make statistically reliable projections for the Department.
- Prior anecdotal information that a sizable percentage of the IA workforce were not IA professionals was confirmed by the data call.
- Prior anecdotal information that a sizable percentage of the IA workforce received little more than on-the-job training was confirmed by the data call.

2. Workforce Management

2.1 Findings and Recommendations

2.1.1 Finding: The CINCs, Services, and Agencies lack necessary capabilities to adequately manage the IT workforce as a whole, and the IA workforce in particular.

Recommendation 1: Direct the OUSD (P&R) to establish the requirement that the CINCs, Services, and Agencies identify manpower and personnel assigned IT/IA functions, enter the required information into the appropriate databases, and maintain these databases as changes occur. (A review is currently being conducted by the Office of Personnel Management (OPM) of IT workforce functions to more accurately define, classify, and track IT positions and personnel. During the execution of Recommendation 1, the results of the OPM efforts can be incorporated since it will also require the identification and review of IT functions, positions, and personnel.)

This includes military, both active and Reserve components, and civilians. Modifications to existing manpower and personnel databases, as well as changes to Service/Agency directives, will be required. (Appendix G outlines the coding requirements.)

2.1.2 Finding: The current trend towards outsourcing IT and IA functions raises concerns regarding potential risks to our mission.

Recommendation 2: Direct the OASD (C3I) to work with the OUSD (A&T) and the OUSD (P&R), as part of the Inherently Governmental Working Group (IGWG), to revise IT function codes and develop definitions that more accurately reflect today's IT and IA activities.

The function codes and definitions will be used by the DoD Components during the next annual Inherently Governmental and Commercial Activities Inventory.

Recommendation 3: Direct the OASD (C3I) to draft guidance for review by the Inherently Governmental Working Group to be used by the DoD Components to determine core IT and IA requirements to minimize the risk of losing mission capability.

Once this core requirement has been defined and quantified, take steps to ensure that this capability is protected from outsourcing.

Recommendation 4: Direct the OUSD (A&T) to consider the merits of developing and maintaining a database that shows contractor staff-years against major functions, especially IT and IA.

2.1.3 Finding: Each of the Services is increasingly challenged in its retention of experienced military IT personnel.

Recommendation 5: Direct the ODASD (MPP) to establish a steering group comprised of OSD, Joint Staff, and each of the Services (including the Coast Guard) to focus on military IT personnel issues.

2.1.4 Finding: The civilian personnel management and compensation flexibilities authorized by the Office of Personnel Management are not being aggressively pursued by organizations plagued with IT shortages.

Recommendation 6: Direct the ODASD (CPP) to work with the ASD (C3I) to widely publicize OPM flexibilities available to address civilian IT recruiting and retention problems.

2.2 Discussion and Analysis

It is clear that if the Department is to develop and maintain a world-class IT workforce, it must first be able to systematically and continually identify and quantify its IT workforce requirements and its existing IT workforce. This capability must be institutionalized within the Department. Existing manpower and personnel databases must be modified to provide this capability. In the meantime, there are several steps the Department can take to address IT workforce issues. The Department should ensure that there is a broad understanding of what capabilities already exist to address recruiting and retention problems for the civilian IT workforce. The Services should continue to aggressively manage their military IT occupational specialties. The Department should rethink its outsourcing policies in IT and begin by changing the IT functional definitions in the Inherently Governmental and Commercial Activities Inventory and providing guidance regarding the maintenance of a core capability.

2.2.1 Military IT Occupational Specialties

Each of the Services has established military IT occupational specialties. DoD-wide, these specialties number approximately 11,000 officers and 38,000 enlisted. These occupational specialties are actively managed by the Services, and there are personnel policies in place to govern the IT professionals. Overall, the Services are meeting end-strength requirements but are increasingly challenged to retain personnel in the IT career specialties. While retention of military personnel in general is currently a concern in the Department, there are some IT-specific occupational specialties, particularly within the Air Force and Marine Corps, where retention has not met expectations and is a concern. Reasons cited for personnel leaving the military include private sector opportunities, PERSTEMPO/OPTempo, and, in some cases, career progression limitations.

Each of the Services has implemented actions to boost retention. These incentives include offering selective reenlistment bonuses, adjusting career fields to improve career progression opportunities, increasing emphasis on continuing education tied to increased Service commitments, and providing commercial certification, again tied to increased Service

commitments. Additionally the Services are increasingly allowing those personnel not selected for advancement to stay in the military past traditional separation gates.

The Services are also encouraging personnel to laterally convert from other specialties into IT specialties and recruiting personnel with prior service experience, subject to specific guidelines, to assist in meeting end-strength requirements.

Each Service is closely monitoring and managing its accession programs to meet end-strength requirements. The Services use computer models that identify specific skill requirements. In some cases, the Services are increasing accessions of personnel into IT specialties to build a larger base population of IT specialties. In other cases, enlistment bonuses are being used to attract personnel into the IT specialties.

Each of the Services changed its officer and enlisted IT career fields in the last three years. These changes include merging specialties, reshaping assignments, improving career progression opportunities, and redefining training requirements and progression, resulting in an improved comprehensive career management plan. The effects of these changes on the overall IT retention effort cannot be assessed at this time. Detailed information on these career fields is available in Appendix F.

While the Services have recognized the problems in retaining experienced military IT professionals and are taking actions to address the problems, many of the approaches are not being shared among the Services. Furthermore, given the long-term situation in the private sector, the Services' retention challenges are not likely to disappear soon. The recommendation to establish an OSD-sponsored steering group would serve to:

- Foster a mutual exchange of information on accession/retention programs related to the military IT professionals,
- Provide a venue for developing new approaches (e.g., commercial certification incentives in exchange for additional service commitments),
- Focus budgeting strategies (e.g., Selective Reenlistment Bonuses (SRBs), enlistment bonuses), and
- Develop long-term military IT personnel strategies.

2.2.2 Outsourcing

We have not had the opportunity to define the functions that are inherently governmental. Given the new awareness of asymmetric threats, we need to analyze more carefully the risks associated with using the non-federal workforce to perform functions that are key to our success on the battlefield. Some of these functions require dealing with very complex products whose very nature makes it easy to disguise flaws. It is critical that we construct our management approach to minimize our vulnerability to these hidden risks. The Department must ensure that some level of core IT and IA capability is maintained or, as a minimum, understand the risks—and their consequences— of losing this core capability.

The IPT was unable to find a data source to identify the number of contractor staff-years currently used in the Department for IT functions. However, using data collected through

the Inherently Governmental and Commercial Activities Inventory Report, the Services and Agencies reported an inventory of almost 101,000 authorized military and civilians for IT functions. Since this Inventory Report does not define its functional categories, the IPT identified those categories in the Inventory Report that best matched the IT functions listed in the Clinger-Cohen competencies.

Out of the inventory identified as IT functions, the Services and Agencies identified almost 29% as subject to review for outsourcing. We know that a substantial part of the IT workload is already assigned to contractors. This means that the potential government's share of the government-contractor split is much less than 70%. What that share should be is a subject of concern, an issue that should be examined sooner, rather than later. The Department must assess the potential risks of losing our in-house capability and take steps to protect a core capability.

Currently, there is inadequate information available regarding contractor work-years used for IT functions. To fulfill a congressional reporting requirement, each year the OUSD (A&T) collects information describing the contractor work-years that support certain high-level functions. Labor expended to support purely IT functions is categorized as such at a general level, but the classification system does not allow visibility into the IT support provided to the line functions such as health services, depot repair, and so forth.

2.2.3 Civilian IT Personnel Management

Although civilian IT shortages cannot be documented at the Department level, IT recruiting and retention difficulties are being experienced at the local levels within the Department. Statistics are available that document the use of recruiting bonuses and retention allowances since FY 1997 (Table 2).

Table 2. Incentives – FY1997 Through March 1999

FY	IT Employees Given Recruiting Bonuses	IT Employees Given Retention Allowances
97	24	138
98	52	161
99 (through Mar 99)	25	166

While pay is not the sole incentive for recruitment and retention, it is a factor in the decision-making process. The Department should begin an aggressive campaign to educate the Services and Agencies regarding both compensation and non-compensation flexibilities available.

3. Training and Certification

3.1 IT Management Training: Findings and Recommendations

3.1.1 Finding: The IT educational programs offered by the Information Resources Management College (IRMC), a part of the National Defense University (NDU), are not being fully utilized by the Department to educate and train IT management professionals or functional personnel with information technology management responsibilities.

Recommendation 7: Direct the OASD (C3I) to require the staffs of the DoD CIOs at the GS-13 through the GS-15 levels to complete the DoD CIO Certificate Program or the Advanced Management Program at the IRMC. Components that wish to use ITM training programs other than IRMC will submit verification of equivalency to the DCIO office to ensure training programs cover mandatory requirements of the Clinger-Cohen Act and the Department's implementation strategies.

Recommendation 8: Direct the OUSD (P&R) and the OASD (C3I) to issue policy directing the Services/Agencies to implement a mandatory requirement that DoD CIOs, Deputy CIOs, and SESs and flag officers on the CIO staffs attend DoD-sponsored ITM executive sessions.

Recommendation 9: Direct the OUSD (Comptroller) to provide resources (personnel and funding) to the IRMC to accommodate additional training requirements of the DoD ITM workforce.

Funds will be used to execute (1) education and training initiatives outlined in this document; (2) the conversion of classroom courses to distance learning to meet the increase in throughput of students; and (3) the development of new ITM education and training requirements (e.g., development of IA Certificate Program for managers).

3.1.2 Finding: DoD does not have a method to continuously educate and train its senior executives, military or civilian, to ensure they are equipped with the necessary knowledge and skills to make effective decisions that impact IT initiatives within their mission areas.

Recommendation 10: Direct the OASD (C3I) to work with the Joint Staff and the ODASD (CPP) to develop an IT contemporary issues training module for the CAPSTONE and APEX training sessions.

3.2 IT Management Training: Discussion and Analysis

The IT workforce is assigned such a wide range of functions that to evaluate IT training in the time frame available would have been an insurmountable task. Rather, the IPT

examined, in general, the existence of IT training in the Department for both the IT professional and the general user. The objective of this review was to identify major gaps in available IT training. Because of the risk to the Department's computer security infrastructure, the primary focus of a detailed examination of IT training was on information assurance, addressed in Section 3.3. IT training, because of the pervasiveness of the technology and the interoperability of systems and networks, is needed by everyone, at least to some degree. The IPT found IT training coverage existed as follows:

- Skill training for the military IT workforce in IT occupational career fields is generally recognized as meeting the needs of the Services.
- Graduate education in the IT field exists both in-house and at colleges and universities around the country, and is used extensively by the Services and Agencies for both military and civilian IT professionals.
- The Services have either already incorporated, or are in the process of doing so, basic IT training and awareness into accession programs for military personnel, such as Reserved Officer Training Corps (ROTC), Officer Candidate School (OCS), Service Academies, and initial skill training courses for non-IT occupational specialties.

The Department spends nearly 1% of its civilian payroll budget on civilian training, which equates to approximately \$750 per person annually. We have no way of determining how much of the expenditure is IT related. However, due to the increase in the use of information technology, training in information technology management should be a priority to maintain skilled personnel to carry out the mission critical functions of the Department. In the private sector, those successful IT organizations with the highest training expenditures measure training investments as a percentage of total payroll. One company, with significant expenditures per employee, spends 15.3% of its payroll on training. In comparison with the private sector, the Department's 1% does not seem sufficient.

Because of the rapid advances in IT, training must be viewed as a continuum designed to maintain a knowledge and skill base that is highly perishable—it is not a one-time career event. This training continuum is critical to sustaining information superiority. Studies and reviews have proven that most system failures result from poor program management and oversight rather than technical problems. Functional managers, sponsors, program and project managers must be skilled enough to strategically plan projects successfully and use management controls that are available to assist in directing information technology initiatives. Section 5125(c)(3) of the Clinger-Cohen Act recognizes the importance of these skills. This act directs federal agencies to define core skill requirements and design programs to rectify deficiencies accordingly.

To meet these requirements, the Federal Chief Information Officer Council approved the Clinger-Cohen Core Competencies to:

- Serve as the federal "requirements established" for personnel,
- Be used as a baseline to assess the skill and knowledge requirements of employees,
- Serve as a tool in human resource planning and management, and

- Serve as a baseline to determine required course and curriculum training requirements in the information resources management field.
- The recommendations in this report are consistent with the requirements of the Clinger-Cohen Act.

The Secretary of Defense named the Information Resources Management College (IRMC) as the primary source of education to meet the training needs of DoD CIOs, executives, and senior-level managers, as required by the Clinger-Cohen Act. Essentially, these programs are encouraged; however, few incentives exist to take full advantage of them.

The DoD CIO also sponsors annual DoD CIO Executive Training Sessions at the IRMC that focus on current critical issues and initiatives in IT. The sessions are intended to provide an awareness of emerging management strategies to address these issues within DoD and private sectors. These sessions are designed for DoD CIOs, Deputy CIOs, and other senior executives. DoD underutilizes these sessions while the other federal agencies have responded overwhelmingly.

If, in the future, the Department decides that a centralized career management program for IT professionals is required, all IT training should be examined. This review should assess how training should be used throughout the IT professional's career and determine the sufficiency and adequacy of the training content and availability. In the meantime, the IRMC Certificate Program should be required for all IT professionals assigned to CIO staffs at the GS-13 level and above. Also, DoD CIOs, Deputy CIOs, and Senior Executive Service (SES) personnel on the CIO staffs should be required to attend annual DoD-sponsored Executive Sessions. To accommodate the increase in throughput of students, additional resources (personnel and funds) must be allocated to the IRMC.

The most important segment of the Department's workforce that requires IT awareness training is the senior leadership: flag and general officers and the SES. These are the individuals who shape the priorities and make decisions that impact IT initiatives within their mission areas. Not knowing the capabilities, limitations, or regulatory requirements regarding IT initiatives puts the Department at risk for additional problems. The Department must ensure that adequate skills, knowledge, and awareness of IT are woven throughout the organization and not just at the IT functional levels. We must seize every opportunity to ensure that the Department's decision makers are briefed, trained, and educated to heighten the IT skill and knowledge capabilities at all levels. Accordingly, the IPT reviewed the CAPSTONE and APEX Programs to ensure key critical competency areas of information technology were addressed.

All general and flag officers are required to attend the six-week CAPSTONE Program at the National Defense University within two years of promotion to general or flag rank. Although there is a substantial portion of the curriculum dedicated to C4I subject areas, the emphasis is on intelligence and information warfare. There is no realistic method to ensure that the high profile, contemporary IT issues are presented to this group within the current curriculum. Currently, OSD senior executives in acquisition, public affairs, and Reserve Affairs each spend approximately 1.25 hours addressing the CAPSTONE students on the "hot" topics in these areas. If each of these three speakers gave up 15 minutes of the

allotted time, 45 minutes would be available for the ASD (C3I) to present the “hot” topics in IT.

The IPT also found that all newly appointed SES members (career and non-career) are required to attend the two-week APEX course. The current curriculum provides no training in contemporary IT issues. These Senior Executives need this training. The APEX course should allocate 45 minutes for the ASD (C3I) to present the “hot” topics in IT.

3.3 IA Training: Findings and Conclusions

3.3.1 Finding: JV 2010 requirements for information superiority, coupled with the Department’s interoperable systems and networks, demand a common language and common baseline of training requirements.

Recommendation 11: Direct the OASD (C3I) to officially adopt NSTISSI Number 4009, *National Information Systems Security (INFOSEC) Glossary*, as the official IA Glossary. This requires the Defense-wide Information Assurance Program (DIAP) to formally coordinate an annex defining terminology not yet officially adopted by NSTISSI but used by the Department.

Recommendation 12: Direct the Joint Staff to review the defensive information operations requirements in the context of JV 2010 and translate these requirements into the Universal Joint Task List (UJTL) and the Joint Mission Essential Task List (JMETL).

3.3.2 Finding: The “critical” IA functions, namely those that require privileged access, should not be assigned to the computer “hobbyist” with minimal to no formal training.

Recommendation 13: Direct the OASD (C3I) to officially adopt the NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* and the NSTISSIs as the minimum DoD IA training standards.

Recommendation 14: Direct the OUSD (P&R) and the OASD (C3I) to establish the requirement that the CINCs, Services, and Agencies establish mandatory training and/or certification programs for the five “critical” IA functions, using the NSTISSC training standards and the IPT-developed certification requirements as the minimum requirement. In support of this, DISA shall develop baseline IA training courses to meet the IA training requirements stipulated in the IPT certification documents. These courses can then be used by the Services and Agencies to meet the certification IA training requirement or enhanced by the Service and Agency to meet its unique needs.

Recommendation 15: Direct the OASD (C3I) to establish the requirement that no person assigned to a “critical” IA function at the entry level may be granted privileged access until the required IA training is successfully completed.

Recommendation 16: Direct the OUSD (P&R) and the OASD (C3I) to establish the requirement that the CINCs, Services, and Agencies document these certification programs in full and develop the capability to readily produce detailed answers about the status of certifications.

Recommendation 17: Direct the OUSD (P&R) and the OASD (C3I), in concert with the CINCs, Services, and Agencies, to coordinate biennial reviews of each certification and/or training program to ensure the currency and utility of the requirements.

3.3.3 Finding: For the most part, IA training is currently provided in a conventional classroom situation.

Recommendation 18: Direct the OUSD (P&R) and the OASD (C3I) to develop and establish an Advanced Distributed Learning program, including a certification management system, for IA training and education at DISA or other appropriate location. The IA Advanced Distributed Learning effort will support implementation of an IA element within the Federal Center for Information Technology Excellence proposed under PDD 63.

This effort must be fully integrated with the manpower, personnel, and training systems of the warfighter. The appropriate DoD, Guard and Reserve Components, and the nation’s academic and training communities must be engaged in this effort. A specific program element should be established to fund development and implementation of this effort. Provisions must be included in the design of this system to ensure availability for our sea-going personnel. Web access is not always available for these personnel.

3.3.4 Finding: With an increasing contractor IA workforce, it is important to ensure that this segment of our workforce does not become the weak link in protecting our information systems. The Department must ensure that contractors are subject to the same training and certification requirements as its own personnel.

Recommendation 19: Direct the OASD (C3I) to incorporate into the DODD 8500.xx, *Information Assurance*, the requirement for contractors assigned “critical” IA functions to meet the same or equivalent certification and training requirements as Department personnel. This recommendation requires that the OUSD (A&T) provide guidance to Contracting Officers to ensure these requirements are included in affected contracts.

3.4 IA Training: Discussion and Analysis

Information superiority in the Department depends on a properly trained IA workforce. Because of the rapid advances in IT, training must be viewed as a continuum designed to maintain a knowledge and skill base that is highly perishable; it is not a one-time career event. This training continuum is critical to sustaining information superiority as required by JV 2010.

The Department's joint warfighting capability in the information age is extremely vulnerable due to the interconnectedness of its information infrastructures. The integrity and availability of our network is critical to ensuring and sustaining information superiority. Our vulnerabilities include:

- Lack of a common IA "language" even among the IA professionals.
- Lack of common training standards.
- Lack of assurance that the Department's IA workforce, particularly those with privileged access, are held to some minimal training requirements before being given the "keys to the kingdom."
- Lack of a consistent capability of Services and Agencies to provide initial skill training to all members of the IA workforce, much less continuing training to maintain currency with the rapidly changing technology.
- Difficulty of maintaining currency of training curricula.

The next step, after identifying training gaps, would normally be to determine training shortfalls. Although the IPT could identify training capacities, it could not identify training required, again because there is no mechanism in place to identify the workforce.

3.4.1 Training and Certification

Implementation of JV 2010 demands information superiority and a joint warfighting capability in a highly networked environment. Existing training standards have the potential to render information systems vulnerable from the uneven skills and abilities of those workers who require critical IA skills. The Department must ensure that training standards are consistent across Services and Agencies, particularly in the skills required to protect the availability and integrity of our information systems.

Although JV 2010 and the Concept for Future Joint Operations both clearly identify the need for information superiority, the concept of *information superiority* is relatively new. There are ongoing efforts to define information superiority in terms of mission accomplishment. The documents used by the warfighter include the UJTL and the JMETL.

A review of these documents reveals that the current focus is almost exclusively on *offensive* information operations. Although the JV 2010 and the Concept for Future Joint Operations address the requirement for DoD-wide "information system/protect skills" or *defensive* information operations, this requirement has yet to be translated into a UJTL or JMETL requirement. If the warfighter is to recognize the critical importance to mission capability and readiness, the requirement must be clearly delineated in those documents of importance to the warfighter—the UJTL and JMETL.

Services and Agencies provided a list of current IA training. IPT analysis of this information showed the following:

- All Services and NSA, DIA, and DISA provide a full range of IA training courses to their system and network administrators. Some of these courses are vendor

provided, some are computer based; some are mobile; most are in a fixed location in a classroom.

- All Services and NSA, DIA, DISA and Defense Logistics Agency (DLA) provide IA training for Information System Security Managers (ISSMs) and Information System Security Officers (ISSOs).
- Only the Army offered a formal training course for Computer Emergency Response Teams (CERT).
- The Air Force provides formal in-house CERT training to members of the Air Force CERT and its quick-reaction teams, separate from its official resident training programs.
- DISA is developing a computer-based CERT course targeting managers. Once this managers' course is completed, a technical CERT training course is scheduled for development.
- No formal training is currently available for individuals on Red Teams or who provide vulnerability or threat assessments. NSA has related vulnerability and threat assessment courses but from an *offensive*, rather than *defensive*, perspective. The Defense Information Systems Agency (DISA) is developing a hands-on exercise, using computer-based training (CBT), to teach systems administrators and managers techniques to reduce threat and vulnerabilities to their information systems.

As efforts proceeded to develop certification and training requirements, it was clear that there was not a common IA language, even among the IA functional experts. Without such a common language, time must be devoted to develop and agree on definitions before IA issues can be resolved. This lack of common terminology can have devastating consequences for a joint warfighting effort. The Department participates in the development of NSTISSI Number 4009, *National Information Systems Security (INFOSEC) Glossary*. The Department should formally adopt this document; the DIAP should coordinate with NSTISSI on the development, maintenance, and publishing of an annex to NSTISSI Number 4009 for DoD IA terminology not yet adopted by NSTISSI; and the DIAP should ensure that subordinate documents are consistent with these two documents.

The IPT focused its IA training efforts on five "critical" IA functions because these functions entail the highest risk:

- System/Network Administration and Operations
- Computer/Network Crime
- Threat and Vulnerability Assessment
- Computer Emergency Response Team (CERT)
- Web Security

This does not mean that remaining functions do not carry a level of risk in the performance of the functions. It does mean that the "critical" functions pose a significantly greater level of risk because of the privileged access. Since the people assigned to these functions are given the "keys to the kingdom," they are the ones that should be the most capable of

protecting the availability and integrity of our information systems, thereby ensuring our information superiority. These same people can put our information systems into a highly vulnerable state, either deliberately, or more likely, inadvertently because they are not properly trained. If the Department is serious about information superiority, it must be equally serious about the high standards it sets for these IA personnel. Technology helps them do the job, but training keeps them prepared to use the existing and emerging tools of technology effectively and appropriately.

It is essential that these certification requirements are consistent, equivalent, and transferable across Services and Agencies. In a joint environment, the Department cannot afford to give its warfighters anything less. In this regard, DISA should be tasked to develop baseline IA training to meet recommended certification training requirements across the Department. CINCs, Services, and Agencies can then use these baselines when determining their Title 10 training requirements.

Training alone was not considered a sufficient criterion to optimize the security of our information systems. Instead, the IPT determined that since information assurance is a core competency and capability essential for achieving information superiority, a process of formal certification using common Department standards was a critical requirement, especially for these five functions. This process begins with formal classroom or computer-based training followed by a period of observed performance demonstrating competence in specific knowledge, skills, and abilities. It requires an official designation of this competency through documented certification and approval by the local commander. Because of the short shelf life of IA technology, certification has a limited validity period; therefore, re-certification is required to keep knowledge and skills current.

The IPT did not address certification and/or training requirements for either the Computer/Network Crime or the Web Security functions since these were already under development. In the case of Computer/Network Crime, a 1998 memorandum¹ from DEPSECDEF tasked the Air Force to act as executive agent for the Department to develop training requirements. In the case of Web Security, another DEPSECDEF memorandum² in the same year chartered a separate IPT to develop certification and training requirements.

Appendices H, I, and J contain the IPT certification requirements for the remaining three “critical” functions: System/Network Administration and Operations, Threat and Vulnerability Assessment, and CERT, respectively. These certification documents are based on NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, and the NSTISSC National Training Standard Instructions. Although the DoD has invested much effort in the development of these NIST requirements and NSTISSC standards, they currently are applicable only to the federal national security community since the DoD has not formally adopted them. Further, the

¹ Department of Defense, Deputy Secretary of Defense, Department of Defense Reform Initiative Directive #27 — DoD Computer Forensics Laboratory and Training Program, February 10, 1998.

² Department of Defense, Deputy Secretary of Defense, *Information Vulnerability and the World Wide Web*, September 24, 1998.

IPT's certification documents include additional specific DoD operational performance needs.

The certification requirements outlined in Appendices H through J have certain prerequisites stipulated. Specifically, background investigations and specific IA training requirements and/or other certification requirements are listed. It is important that Services and Agencies recognize that the intent of the IPT was that these prerequisites must be met before the individual is granted privileged access.

3.4.2 Contractor Certification Requirements

Contractors are performing many "critical" IA functions. Their effort is expected to increase for a variety of reasons. However, because of the concerns about protecting the Department's networks and ensuring properly trained and certified personnel, contractor personnel must be held to the same or equivalent standards as government personnel. Contractual provisions are available for defining standards that must be met by contractor personnel. Certification requirements can be included as an attachment to the Statement of Work (SOW), and contractors can be instructed to identify those personnel proposed for "privileged access" via a Key Personnel clause. This method requires governmental approval for individual(s) proposed, and maintains the contractual right to approval for any subsequent replacement personnel. Certification of contractor personnel at the required levels of expertise would then take place at the time of the contract award.

3.4.3 Long-Term IA Training Initiative

The long-term viability and capability of our IA workforce is a strategic IA element in achieving information superiority.

DoD Components have a number of IA-related training courses underway and in development, but each of these has limitations that impact the Department's readiness to respond decisively and effectively to information system attacks. A more efficient and effective way is needed to train, assess, and certify DoD personnel in "critical" IA knowledge and skills.

The Defense Acquisition University (DAU) has demonstrated how high-quality Web-based training can be provided to DoD personnel anytime and anywhere. DAU has invested in software to manage students (while taking courses online) that can be quickly adapted for IA training and implemented by other training providers.

Adopting a Web-based training approach and an associated management information system would enable the Department to quickly develop, distribute, and manage IA training across the DoD. This training approach is particularly well suited to support the unique demands on the Department's Reserve Components. It would reduce the time and cost associated with travelling to and maintaining a classroom and/or platform training. It would establish common learning objectives and performance standards relating to specific occupations and skill levels. It would provide a means to quickly update and distribute IA-related information to specific personnel at their job sites whenever needed. And it would reduce the cost of redundant course development effort underway in each Component.

The President's Executive Order 13111 of January 1999 tasked the federal agencies with increasing the use of learning technology to enhance the cost-effectiveness of federal education and training. In keeping with the intent of this Executive Order, DoD should launch a Web-based IA training program in collaboration with the other federal agencies. This effort would reduce the cost of DoD's investment while simultaneously enhancing the readiness of all federal network and information systems.

4. Roadmap to Improvements

4.1 Implementing the IPT Recommendations

Previous chapters presented the IPT's recommendations. These recommendations, when fully implemented, will significantly improve the Department's capability to meet the JV 2010 goal of information superiority. What the Department will accomplish is depicted in Table 3.

Table 3. Anticipated Results and Implementation Status

If the DoD Implements...	The Results Would Be...	Projected or Current Status
Recomm. 1	The Department's IT and IA workforces, both authorized billets and positions and personnel, will be able to be systematically and continually identified and quantified. This capability will be institutionalized.	Implementation in the mode of "business-as-usual" will require about three years once funding is provided. If sufficient priority is given to this recommendation, completion could be realized in about 18 to 24 months.
Recomms. 2, 3, and 4	The Department will have more accurate information about its government and contractor mix in the IT/IA workforce. A mechanism will be in place to maintain a core capability in these critical functions and to assess the risk of additional outsourcing.	Work is being currently initiated in these areas. By next year, information will be available to begin examination of outsourcing issues and risks.
Recomm. 5	The Department will have a forum for Services' military IT career managers to identify and assess improved methods for managing their people.	Implementation could be completed within three months or less and continue as long as the shortage of IT personnel is a serious problem.
Recomm. 6	Local commanders and directors will have better information on already-approved civilian personnel management capabilities to improve their ability to recruit and retain civilian IT professionals.	Implementation can be completed within three months. The use of recruiting bonuses and retention allowances can be tracked on a regular basis.
Recomms. 7, 8, 9, and 10	IT training for the Department's senior executives (military and civilians) and CIO staffs will meet the requirements of the Clinger-Cohen Act.	CIO staff training can begin immediately. However, funding is necessary to accommodate additional throughput of students and the development of course and curricula to address new IT training requirements.
Recomms. 11, 12, and 13	The Department will have a common IA language, a common reference point for joint training requirements, and a	Adoption of the NSTISSI Glossary and training standards can be implemented within three months. Development of a

If the DoD Implements...	The Results Would Be...	Projected or Current Status
	baseline IA training standard.	DoD Glossary supplement and UJTL and JMETL modifications can be implemented within six months.
Recomms. 14, 15, and 17	The Department will have increased assurance about the reliability of the IA workforce and its ability to protect the integrity and availability of the Department's interoperable and networked information systems. An institutionalized certification process will replace today's non-existent standards, including maintaining the currency of the standards.	Although full implementation will require three to five years once funding is provided, substantial progress can be achieved annually if appropriate priority is given to the effort.
Recomms. 16 and 18	The Department will have the capability to maintain current IA training modules and deliver this training to the workforce in a timely and cost-effective manner as well as track the currency of the workforce's certification.	Although it will take five years to fully implement these recommendations, by capitalizing on similar work already completed, the requirements can be prioritized, with specific capabilities completed progressively beginning with the first year after funding is provided.
Recomm. 19	The Department's IT/IA contractors will meet the same minimum training and certification requirements as our military personnel and civilian employees.	The policy can be promulgated within six months. All new contracts would meet the requirements from the time the policy was promulgated. Estimates are up to two years before all existing contracts requiring changes are amended.

4.2 Priorities

The nineteen recommendations are grouped into four priorities: 1, 2, 3, and 4.

- **Priority 1** recommendations are those which have a direct impact on substantially improving the Department's ability to protect the integrity and availability of its information systems and networks and its ability to operate effectively in a joint warfighting environment. *Recommendations 14, 15, and 19.*
- **Priority 2** recommendations are those which enable the Department to substantially improve its ability to manage its IT workforce or which provide long-term efficiencies for Priority 1 recommendations. *Recommendations 1, 2, 3, 6, 10, and 18.*
- **Priority 3** recommendations are those which enable the Department to improve the quality of its IT workforce and maintain improvements realized as a result of implementing Priority 1 recommendations. *Recommendations 5, 7, 8, 9, 16, and 17.*
- **Priority 4** recommendations are those which will provide official policy guidance to support the recommendations above. *Recommendations 4, 11, 12, and 13*

4.3 Costs

These recommendations are not without cost. The IPT's recommendations are listed in Table 4 on page 26, along with the costs to implement. Approving the recommendations will not result in implementation, simply another unfunded requirement. Appropriate dollars must be provided. To fully fund these recommendations will require \$77.5 million over the next five years. Once the recommendations are approved and the dollars provided in the budget, the timelines shown in the next section can commence. See Appendix K for Service and Agency cost breakouts.

4.4 Timeline for Implementation

The timeline shown in Appendix L begins with Month 0. Month 0 is defined to be that month in which implementation is directed and, when required, dollars are provided.

4.5 Future Issues to be Addressed by OSD

There are a number of issues left unresolved due to a lack of personnel data. Once Recommendation 1 is fully implemented, the workforce needs to be analyzed and management alternatives examined with respect to:

- The impact of the non-IT professional assigned IT functions;
- The size and distribution of the civilian IT professional workforce and the desirability of a career management program for that workforce; and
- Recruiting and retention statistics for the civilian IT workforce and identification of required management actions.

There are two additional issues that should be considered for additional work:

- Certification requirements should be developed for the non-critical IA functions.
- Staffing guidelines for manpower-intensive IA functions should be developed using independent variable(s) that can be easily determined during the program/budget process.

Table 4. IPT Recommendations and Their Costs

Recommendation	Page	Cost
Recommendation 1: Direct the OUSD (P&R) to establish the requirement that the CINCs, Services, and Agencies identify manpower and personnel assigned IT/IA functions, enter the required information into the appropriate databases, and maintain these databases as changes occur.	9	\$12.5M
Recommendation 2: Direct the OASD (C3I) to work with the OUSD (A&T) and the OUSD (P&R), as part of the Inherently Governmental Working Group (IGWG), to revise IT function codes and develop definitions that more accurately reflect today's IT and IA activities.	9	No cost
Recommendation 3: Direct the OASD (C3I) to draft guidance for review by the Inherently Governmental Working Group to be used by the DoD Components to determine core IT and IA requirements to minimize the risk of losing mission capability.	9	No cost
Recommendation 4: Direct the OUSD (A&T) to consider the merits of developing and maintaining a database that shows contractor staff-years against major functions, especially IT and IA.	9	No cost
Recommendation 5: Direct the ODASD (MPP) to establish a steering group comprised of OSD, Joint Staff, and each of the Services (including the Coast Guard) to focus on military IT personnel issues.	10	No cost
Recommendation 6: Direct the ODASD (CPP) to work with the ASD (C3I) to widely publicize OPM flexibilities available to address civilian IT recruiting and retention problems.	13	No cost
Recommendation 7: Direct the OASD (C3I) to require the staffs of the DoD CIOs at the GS-13 through the GS-15 levels to complete the DoD CIO Certificate Program or the Advanced Management Program at the IRMC.	13	See Recomm. 9
Recommendation 8: Direct the OUSD (P&R) and the OASD (C3I) to issue policy directing the Services/Agencies to implement a mandatory requirement that DoD CIOs, Deputy CIOs, and SESs and flag officers on the CIO staffs attend DoD-sponsored ITM executive sessions.	13	See Recomm. 9
Recommendation 9: Direct the OUSD (Comptroller) to provide resources (personnel and funding) to the IRMC to accommodate additional training requirements of the DoD ITM workforce.	11	\$5.8M
Recommendation 10: Direct the OASD (C3I) to work with the Joint Staff and the ODASD (CPP) to develop an IT contemporary issues training module for the CAPSTONE and APEX training sessions.	13	No cost
Recommendation 11: Direct the OASD (C3I) to officially adopt NSTISSI Number 4009, National Information Systems Security (INFOSEC) Glossary, as the official IA Glossary. This requires the Defense-wide Information Assurance Program (DIAP) to formally coordinate an annex defining terminology not yet officially adopted by NSTISSI but used by the Department.	16	No cost
Recommendation 12: Direct the Joint Staff to review the defensive information operations requirements in the context of JV 2010 and translate these requirements into the Universal Joint Task List (UJTL) and the Joint Mission Essential Task List (JMETL).	20	No cost

4. Roadmap to Improvements

Recommendation	Page	Cost
Recommendation 13: Direct the OASD (C3I) to officially adopt the NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model and the NSTISSIs as the minimum DoD IA training standards.	16	No cost
Recommendation 14: Direct the OUSD (P&R) and the OASD (C3I) to establish the requirement that the CINCs, Services, and Agencies establish mandatory training and/or certification programs for the five “critical” IA functions, using the NSTISSC training standards and the IPT-developed certification requirements as the minimum requirement. In support of this, DISA shall develop baseline IA training courses to meet the IA training requirements stipulated in the IPT certification documents. These courses can then be used by the Services and Agencies to meet the certification IA training requirement or enhanced by the Service and Agency to meet its unique needs.	16	\$10.5M
Recommendation 15: Direct the OASD (C3I) to establish the requirement that no person assigned to a “critical” IA function at the entry level may be granted privileged access until the required IA training is successfully completed.	17	No cost
Recommendation 16: Direct the OUSD (P&R) and the OASD (C3I) to establish the requirement that the CINCs, Services, and Agencies document these certification programs in full and develop the capability to readily produce detailed answers about the status of certifications.	17	Unknown —should be included in Recomm. 18.
Recommendation 17: Direct the OUSD (P&R) and the OASD (C3I), in concert with the CINCs, Services, and Agencies, to coordinate biennial reviews of each certification and/or training program to ensure the currency and utility of the requirements.	17	No cost
Recommendation 18: Direct the OUSD (P&R) and the OASD (C3I) to develop and establish an Advanced Distributed Learning program, including a certification management system, for IA training and education at DISA or other appropriate location. The IA Advanced Distributed Learning effort will support implementation of an IA element within the Federal Center for Information Technology Excellence proposed under PDD 63.	17	\$49M
Recommendation 19: Direct the OASD (C3I) to incorporate into the DODD 8500.xx, Information Assurance, the requirement for contractors assigned “critical” IA functions to meet the same or equivalent certification and training requirements as Department personnel. This recommendation requires that the OUSD (A&T) provide guidance to Contracting Officers to ensure these requirements are included in affected contracts.	17	Unknown cost — unable to determine at this time

Appendix A. Private Sector Recruiting and Retention Techniques

What are Private Sector IT Recruiting Techniques?	
Compensation	<p>Offer competitive salaries...geographic diversification to lower labor costs</p> <p>Hiring bonuses for top candidates</p> <p>Use contingent workers extensively...lowers cost of pay and benefits</p> <p>Employee Stock Option Plans (ESOP) used extensively at smaller firms</p> <p>Recruits also interested in portable 401(k) plans</p>
Targeted Audience	<p>Pursue graduates from two distinct educational sources:</p> <p>Vocational-Technical schools (like DeVry) for systems administrators</p> <p>Colleges & Universities for engineers, software developers, knowledge workers</p> <p>Variations of <i>Best of the Best</i> program:</p> <p>Recruit at target colleges, 1 year rotational assignments in field & corp. HQ</p> <p>Trainee then chooses preferred assignment and location</p> <p>Smaller firms cannot afford college recruiting, often use corporate headhunters</p>
Recruiting Tools	<p>List website in newspaper, movie theater ads</p> <p>E-mail existing resume or create individualized resume</p> <p>Use <i>cookie technology</i> to trace inquiries</p> <p>Cold calling to potential candidates in competing firms</p> <p>Infiltrate social events, like exchanging business cards at microbrewery festivals, art fairs, home & garden shows</p> <p>Assign candidates an in-house, demographically similar <i>pal</i></p> <p><i>Pals</i> receive referral fee if recruits are hired</p>
Source: Defense Manpower Data Center	

What are Private Sector IT Retention Techniques?	
Job Satisfaction	<p>Provide challenging and rewarding work, clearly defined career progression paths</p> <p>Lowest turnover among engineers and software developers</p> <p>Conduct periodic surveys of attraction & retention trends: Why did you stay/leave?</p>
Compensation	<p>Bonuses can range from 7% (technical support) to 50%+ (key managers)</p> <p>Stock options for star performers...supervisors often given attrition rate ceilings on these major revenue producers</p> <p>Up to \$10K for referring new hires</p> <p>Promise of unlimited potential for financial reward based on firm's profitability</p>
Quality of Life Amenities	<p>More flexible workforce...80 hours of work over 9 workdays, job-sharing, contingent workers, telecommuting</p> <p>Key workers get laptops and Intermediate Service Digital Network lines to homes</p> <p>Extensive equipment and software for telecommuters</p> <p>Typical Silicon Valley QOL package includes workout facilities, dry cleaning services, movie rentals, gourmet cafeterias</p>
Training	<p>Often conducted after normal working hours</p> <p>In-house technical training and fully funded advanced degrees</p> <p>Training needs usually subordinate to quarterly revenue targets</p>
Source: Defense Manpower Data Center	

Appendix B.
Recruiting and Retaining
Information Technology Professionals

RECRUITING AND RETAINING INFORMATION TECHNOLOGY PROFESSIONALS

**Prepared by the U.S. Office of Personnel Management
November 1998**

RECRUITING AND RETAINING INFORMATION TECHNOLOGY PROFESSIONALS

As we move toward the 21st century, it has become increasingly important for the Federal Government to recruit and retain information technology (IT) professionals³ with the skills and competencies needed to meet new technology challenges and remain competitive with the private sector. As agencies develop strategies for recruiting and retaining IT professionals, they will find that a number of existing human resource management flexibilities and resources are available to help address the recruiting and retention problems facing IT managers.

The Office of Personnel Management (OPM) has compiled a list of human resource management approaches and tools that agencies may use in designing IT recruitment and retention strategies and in resolving current staffing problems. This document describes some of the staffing, compensation, award, and training flexibilities that are available to help agencies attract and retain IT professionals, including members of the Senior Executive Service (SES), and describes some of OPM's human resource management initiatives currently under development. In addition, the Appendix provides information on other Federal benefits that may help address employee recruitment and retention issues, such as work life flexibilities and leave, retirement, and insurance benefits. Finally, the Appendix provides a list of OPM contacts for additional information on these flexibilities.

The following pay and benefit options and recruitment tools are important for Federal managers to use as they compete with other employers. Managers of information technology need to know how to use these tools and how they can best be combined to solve particular staffing problems. But the listed tools alone cannot solve the problems of IT worker shortages. The reasons employees choose other employers are many. For example, a study by the placement firm, Blessing-White, suggests that conflict between employees and supervisors is a strong factor in leading IT employees to leave their jobs.

Perhaps the most important factor in attracting and retaining information technology professionals is conscientious and direct involvement by IT managers. Managers need to identify where targeted recruiting efforts are likely to be fruitful. Managers need to be specific in describing the work that is to be done and the competencies that need to be used.

³ Federal information technology positions are typically classified under the General Schedule (GS) in the following series: GS-334, Computer Specialist; GS-391, Telecommunications Specialist; GS-854, Computer Engineering; and GS-1550, Computer Science. The grades of Federal IT positions typically range from GS-5 to GS-15 in such areas as policy, expert, supervision, and management. There are also IT positions in the Senior Executive Service. Occupational series and grade levels vary according to actual duties and responsibilities assigned to specific positions.

Managers need to be creative in “selling” prospective employees on the nature and importance of their agencies’ projects. And managers need to be accomplished in coaching and leading IT employees.

Probably the best way for Federal agencies to resolve their IT recruitment and retention problems is to band together in seeking solutions, relying on the combined insights of managers and personnel lists. An effective way to do this is through an interagency task force, and one has been formed to address this specific issue. Representatives of the Human Resources Technology Council have joined forces with the Education and Training Committee of the Chief Information Officer’s Council to look at specific problems and solutions in IT employee recruitment, retention, development and workforce planning. The task force brings together knowledgeable leaders from OPM, the Office of Management and Budget (OMB), the Interagency Advisory Group of Personnel Directors, the Human Resources Development Council, and the financial and IT communities.

TOOLS AND STRATEGIES

A. Strategies for Recruiting New Employees

For information on additional flexibilities that are available to help recruit new employees, see the Appendix.

1. Agency-Based Flexibilities

The Federal Job Search Process

- This 3-step process begins with Federal agencies listing job opportunities in the USAJOBS Government-wide automated employment information system. Job seekers may access the system in any of the following ways:
 - on the world wide web at <http://www.usajobs.opm.gov>;
 - by electronic bulletin board at 912-757-3100;
 - by telephone at 912-757-3100 (912-744-2299 TDD) or local telephone service available at 17 OPM Service Centers around the country; or
 - touch screen computer kiosks located throughout the nation at OPM offices, Federal buildings, and some colleges and universities.

The USAJOBS systems provide access to over 6000 daily updated job listings, full job announcements, and fact sheets on commonly requested Federal employment topics.

The second step is to review the job announcement to determine eligibility and interest.

The final step in this process is to follow the application instructions. Application for most jobs can be with a resume, the Optional Application for Federal Employment (OF-612), or any other written format. For unique jobs or those filled through automated procedures, special forms and/or instructions may be identified in the job announcement.

Alternative Short-Term Recruitment and Staffing Options

- Use of temporary appointments in the competitive service for positions not expected to last longer than 1 year, but which may be extended for 1 additional year. Recruitment for these positions is accomplished through the competitive process. [5 CFR part 316]
- Use of term appointments in the competitive service when positions are expected to last longer than 1 year, but not more than 4 years. Reasons for making term appointments include project work and extraordinary workloads. Recruitment is accomplished through the competitive process. [5 CFR part 316]
- Making appointments with varying work schedules such as part-time (which may include job-sharing arrangements), intermittent, and seasonal. Intermittent work schedules are used only when the nature of the work is sporadic and unpredictable. Seasonal work involves annually recurring periods of work which is expected to last at least 6 months during a calendar year. The use of varying work schedules may serve as an incentive to attract applicants who prefer to work less than full-time. [5 CFR part 340]
- The excepted service appointment of expert and consultants under 5 U.S.C. 3109 to perform expert or consultant work that is temporary (not to exceed 1 year) or intermittent. (This differs from employing experts and consultants through procurement contracts, which are covered by regulations issued by the General Services Administration.) Under 5 CFR part 304, an expert is someone who is specifically qualified by education and experience to perform difficult and challenging tasks in a particular field beyond the usual range of achievement. A consultant is someone who can provide valuable and pertinent advice generally drawn from a high degree of broad administrative, professional, or technical knowledge or experience. - The appointment of veterans in the excepted service under the Veterans' Readjustment Appointment. This is a special authority under which agencies can appoint an eligible veteran up through the GS-11 or equivalent grade level without competition. The candidate must meet specific service requirements along with the applicable qualification requirements. [5 CFR part 307]
- The appointment of graduate and undergraduate students in the excepted service under the Student Educational Employment Program. There are two components of this program: the Student Temporary Employment Program (STEP) and Student Career Experience Program (SCEP). These are special authorities under which agencies can appoint students who are enrolled or have been accepted for enrollment for at least a part-time schedule at an accredited institution. Appointment in the STEP program is not-to-exceed 1 year, and may not be converted to permanent. Individuals in the SCEP program may be noncompetitively converted to

- career/career-conditional appointments within 120 days of academic requirements completion. Agencies may pay for college courses that improve the performance of students hired under SCEP. In return, the agency may require the student to sign a continued service agreement with the agency.
- A detail within a department of its employees for brief periods. 5 U.S.C. 3341 allows for intra-agency details in increments of 120 days when approved by the head of the department.
 - Commercial temporary help services may be used for brief periods (120 days, with an extension of an additional 120 days) for short-term situations. This option may be used only when regular recruitment and hiring procedures are determined to be impractical, and is accomplished through the Federal procurement system. [5 CFR part 300, subpart E]
 - Agencies may also choose to enter into various types of contracts where appropriate. These contracts are also handled through the Federal procurement system.

Travel and Transportation Expenses for Interviews and/or New Appointments

An agency, at its discretion, may pay the travel or transportation expenses of any individual candidate for a pre-employment interview, or pay travel and transportation expenses for a new appointee to the first post of duty. For either payment, a decision made for one vacancy does not require a like decision for any similar future vacancies. Before authorizing any payments, the agency must consider factors such as availability of funds, desirability of conducting interviews, and feasibility of offering a recruiting incentive. [5 U.S.C. 5706b; 5 CFR part 572]

Superior Qualifications Appointments

Federal agencies have the authority to set pay for new appointments or reappointments of individuals to General Schedule positions above step 1 of the grade based on superior qualifications of the candidate or a special need of the agency. Agencies must have documentation and recordkeeping procedures on making superior qualifications appointments in place in order to make such appointments. [5 U.S.C. 5333; 5 CFR 531.203(b)]

Advancement Opportunities

Employees hired into positions that have been announced as having “promotion potential” to a certain grade level may receive noncompetitive promotions up to that pre-determined level.

Advance Payments for New Appointees

Agencies may advance a new hire up to two paychecks so that a new employee can meet living and other expenses. [5 U.S.C. 5524a; 5 CFR part 550, subpart B]

Use of “Highest Previous Rate”

Upon reemployment, transfer, reassignment, promotion, demotion, or change in type of appointment, agencies have discretionary authority to set the rate of basic pay of an employee by taking into account a rate of basic pay previously received by an individual while employed in another civilian Federal position (with certain exceptions), not to exceed the maximum rate of the employee’s grade. [5 U.S.C. 5334(a); 5 CFR 531.202 (definition of “highest previous rate”) and 531.203(c) & (d)]

Recruitment and Relocation Bonuses

Agencies have discretionary authority to make a lump-sum payment of up to 25 percent of basic pay to a newly appointed employee (in the case of a recruitment bonus) or to an employee who must relocate (in the case of a relocation bonus) to fill a position that would otherwise be difficult to fill. In return, the employee must sign a service agreement with the agency. A recruitment bonus may be used in combination with superior qualifications appointments. Recruitment and relocation bonuses must be paid in accordance with the agency’s previously established recruitment and relocation bonus plans. Recruitment and relocation bonuses are subject to the aggregate limitation on total pay (currently \$151,800). [5 U.S.C. 5753; 5 CFR part 575, subparts A and B]

2. Flexibilities Available with OPM and/or OMB Approval

Special Salary Rates

OPM is authorized to establish higher special rates of pay for an occupation or group of occupations nationwide or in a local area based on a finding that the Government’s recruitment or retention efforts are, or would likely become, significantly handicapped without those higher rates. The minimum rate of a special rate range may exceed the maximum rate of the corresponding grade by as much as 30 percent. However, no special rate may exceed the rate for Executive Level V (currently \$110,700). A special rate request must be submitted to OPM by department headquarters and must be coordinated with other Federal agencies with employees in the same occupational group and geographic area. [5 U.S.C. 5305; 5 CFR part 530, subpart C]

Critical Position Pay Authority

Based on a recommendation from OPM, OMB is authorized to increase the rate of basic pay for a position up to the rate for Executive Level I (currently \$151,800). Critical pay may be authorized for a position that requires expertise of an extremely high level in a scientific, technical, professional, or administrative field or one that is critical to the agency’s successful accomplishment of an important mission. Critical pay may be granted only to the extent necessary to recruit or retain an individual exceptionally well qualified for the position. [5 U.S.C. 5377; OMB Bul. No. 91-09]

B. Strategies for Retaining Current Employees

For information on additional flexibilities that are available to help retain current employees, see the Appendix.

1. Agency-Based Flexibilities

Retention Allowances

Agencies have discretionary authority to make continuing (i.e., biweekly) payments of up to 25 percent of basic pay to individual employees and of up to 10 percent of basic pay to a group or category of employees based upon a determination by the agency that (1) the unusually high or unique qualifications of the employees or a special need of the agency for the employees' services makes it essential to retain the employees, and (2) the employee or a significant number of employees in the targeted category would be likely to leave the Federal Government (for any reason, including retirement) in the absence of a retention allowance. Retention allowances must be paid in accordance with the agency's previously established retention allowance plan and must be reviewed and certified annually. Retention allowances are subject to the aggregate limitation on total pay (currently \$151,800). [5 U.S.C. 5754; 5 CFR part 575, subpart C]

Premium Pay, Exceptions to the Biweekly Limitation

The head of an agency or his or her designee may make an exception to the GS-15, step 10, biweekly limitation on premium pay when he or she determines that an emergency involving a direct threat to life or property exists. If the head of an agency determines that such an emergency exists, the premium pay paid to an employee performing work in connection with that emergency, when added to the employee's rate of basic pay (including any locality payment or special salary rate), must not cause his or her total pay to exceed the rate for GS-15, step 10 (including any locality payment or special salary rate), on an annual basis. [5 U.S.C. 5547(b); 5 CFR 550.106]

OPM encourages agencies to exercise this authority in the case of any employee who performs emergency work to resolve a direct threat to property (including monetary errors or costs) in connection with updating computer systems to prevent malfunction, erroneous computations, or other problems related to the Year 2000 conversion. By exercising this authority in appropriate situations, agencies will be able to ensure that employees who perform significant amounts of overtime work (or work at night, on Sunday, or on a holiday) will be appropriately compensated for that work, as long as the premium pay they receive does not cause their total pay to exceed the rate for GS-15, step 10, on an annual basis.

Use of "Highest Previous Rate"

As previously described in A(1), agencies have the discretion to set pay above the minimum rate of the grade upon transfer, reassignment, promotion, demotion, or

change in type of appointment using the “highest previous rate” authority. [5 U.S.C. 5334(a); 5 CFR 531.202 (definition of “highest previous rate”) and 531.203(c) & (d)]

Granting a “Quality Step Increase”

Agencies have discretionary authority to accelerate an employee’s pay by granting a quality step increase. A quality step increase is an additional step increase that may be granted to an employee who has received the highest rating of record available under the applicable performance appraisal program, which would be “Outstanding” or Level 5 if such a level is available. Employees in agencies which do not have an “Outstanding” level must also meet additional criteria specified by the employing agency. These are basic pay increases for all purposes. No more than one quality step increase can be granted within a 52-week period, and such an increase cannot cause the employee’s pay to exceed the maximum rate of the grade. [5 U.S.C. 5336; 5 CFR part 531, subpart E]

Performance and Incentive Awards

Agencies have discretionary authority to grant an employee a lump-sum cash award based on a “Fully Successful” or better rating of record or in recognition of accomplishments that contribute to the efficiency, economy, or other improvement of Government operations. Awards can be tied to specific achievements such as meeting milestones identified as part of the work needed to achieve Year 2000 conversion goals. Cash awards do not increase an employee’s basic pay. Awards based on the rating of record can be up to 10 percent of salary, or up to 20 percent for exceptional performance, provided the award does not exceed \$10,000 per employee. [5 U.S.C. 4302, 4503, 4505a; 5 CFR 451.104]

2. Flexibilities Available with OPM and/or OMB Approval

Retention Allowances

Upon the request of the head of an agency, OPM may approve a retention allowance in excess of 10 percent, not to exceed 25 percent, of an employee’s rate of basic pay for a group or category of employees based upon a determination by the agency that (1) the unusually high or unique qualifications of the employees or a special need of the agency for the employees’ services makes it essential to retain the employees, and (2) a significant number of employees in the targeted category would be likely to leave the Federal Government (for any reason, including retirement) in the absence of a retention allowance. Retention allowances must be paid in accordance with the agency’s previously established retention allowance plan and must be reviewed and certified annually. Retention allowances are subject to the aggregate limitation on total pay (currently \$151,800). [5 U.S.C. 5754; 5 CFR part 575, subpart C]

Special Salary Rates

As previously described in (A)(2), the special salary rate authority helps agencies retain employees in occupations or geographic areas experiencing a staffing problem. [5 U.S.C. 5305; 5 CFR part 530, subpart C]

Awards Over \$10,000

When agencies exercise the discretionary awards authority described in (B)(1), any award that would grant over \$10,000, up to \$25,000, to an individual employee must first be submitted to OPM for review and approval. Any award that would grant over \$25,000 to an individual employee must be reviewed by OPM for submission to the President for approval.

C. Strategies for Rehiring Former Employees

1. Agency-Based Flexibilities

Use of “Highest Previous Rate”

As previously described (A)(1), agencies have the discretion to set pay above the minimum rate of the grade upon reemployment using the “highest previous rate” authority. [5 U.S.C. 5334(a); 5 CFR 531.202 (definition of “highest previous rate”) and 531.203(c) & (d)]

2. Flexibilities Available with OPM Approval

Waiver of Dual Compensation Restrictions for Reemployment of Military and Civilian Retirees

Laws restricting dual compensation prohibit retired regular military officers of all uniformed services and all Federal civilian retirees from getting the full combined value of their salary and annuity upon reemployment in the Federal service. In addition, for all military retirees the law sets a “pay cap” that limits the combined basic pay plus military retired pay to level V of the Executive Schedule (currently \$110,700).

The Director of OPM may waive the reduction in a retiree's salary or annuity, when an agency encounters exceptional difficulty in recruiting or retaining a qualified candidate for a particular position. Agency heads may ask OPM to waive reductions on a case-by-case basis as described in 5 CFR part 553. In addition, agency heads may ask OPM to delegate waiver authority for temporary positions to deal with “an emergency involving a direct threat of life or property or other unusual circumstances.” Under delegated authority the agency head can provide waivers on a case-by-case basis.

Generally, OPM responds to requests that meet the criteria in 5 CFR 553 within 2 weeks of receipt. The Director of OPM has announced the availability of delegations

and case-by-case waivers for temporary positions working solely on Year 2000 conversion within 24 hours of receipt of an appropriate agency request. [5 U.S.C. 5532(g), 8344(i), and 8468(f); 5 CFR 553]

D. Strategies for Recruiting and Retaining Senior Executives

Many of the strategies used for recruiting and retaining non-executive employees are available for senior executives as well, such as recruitment and relocation bonuses, retention allowances, travel for interviews and/or new appointments, critical pay, incentive awards, work life programs, and benefits. Therefore, this section will highlight those additional flexibilities that pertain specifically to senior executives. Agencies have considerable flexibility for managing their executive resources programs. They may exercise these authorities in accordance with law, OPM regulations, and agency delegations.

1. Agency-Based Flexibilities for the Senior Executive Service (SES)

- Decide how executive positions will be filled (i.e., competitively or noncompetitively) and what recruitment methods will be used. Reassign career appointees to any SES position in the same agency for which qualified with advance written notice. [5 U.S.C. 3132, 3134, 3393, and 3395(a); 5 CFR 317.901]
- Make SES limited emergency appointments (up to 18 months) and limited term appointments (up to 3 years) of career or career-type civil service employees to meet unanticipated temporary staffing needs, without competition, using an authority from the agency's limited appointment pool provided by OPM regulation. [5 U.S.C. 3132 and 3394; 5 CFR 317.601]
- Make career appointments to the SES using merit staffing procedures, after the executive qualifications of the selectee have been approved by an independent Qualifications Review Board. [5 U.S.C. 3393; 5 CFR Part 317, subpart D]
- Set a senior executive's pay at any of the six SES basic pay rates, and adjust that rate once in any 12-month period. [5 U.S.C. 5383(a), (c), and (d); 5 CFR 534.401]
- Pay annual lump-sum performance awards (bonuses) to SES career members, after considering the agency Performance Review Board recommendations. Awards may be between 5 percent and 20 percent of basic pay. [5 U.S.C. 5384; 5 CFR 534.403]
- Pay travel and transportation expenses for career appointees for "last move home." If reassigned or transferred geographically (when eligible for optional or discontinued service retirement or within 5 years of eligibility for optional retirement), career appointees are entitled to moving expenses at retirement. (Implementation regulations are issued by GSA as part of the Federal Travel Regulations.) [5 U.S.C. 5724]

- Individual executives may accumulate up to 90 days (720 hours) of annual leave, which can be carried over from one leave year to the next. [5 U.S.C. 6304; 5 CFR part 630]

2. Flexibilities Available with OPM, OMB, and/or White House Approval

- Make SES limited emergency appointments (up to 18 months) and limited term appointments (up to 3 years) of private sector and other than career or career-type civil service employees to meet unanticipated temporary staffing needs without competition. [5 U.S.C. 3132, 3394; 5 CFR 317.601]
- With White House approval, bestow Presidential Distinguished and Meritorious Rank Awards on SES career appointees for extraordinary executive accomplishment over an extended period. Distinguished Executives receive \$20,000; Meritorious Executives receive \$10,000. [5 U.S.C. 4507; 5 CFR 451.201(c)]

E. Strategies for Using Training and Education to Recruit and Retain Employees

- Paying for Training and Education
 - Agencies can pay for training and education to improve an employee's performance of his or her official duties. With this authority, agencies may pay, or reimburse an employee, for all or part of the necessary expenses of training, including the costs of college courses. [5 U.S.C. 4109(a)(2)]
 - To recruit or retain employees in occupations in which an agency has or anticipates a shortage of qualified personnel, especially in occupations involving critical skills, an agency may pay for education leading to an academic degree. Merit system principles apply to selecting employees for academic degree training. [5 U.S.C. 4107(b); 5 CFR 410.308]
 - Agencies may require service agreements for training of long duration or of high cost. With this authority, agencies protect their investment and secure a period of service from an employee once the employee completes needed training. [5 U.S.C. 4108; 5 CFR 410.309]

- Sharing the Costs of Training and Education

Agencies may share training costs with employees. This authority allows agencies to support training and education that benefits both the agency and the employee. If both agree, an agency may pay some of the costs of training, while the employee pays the balance. An employee may pay the entire cost of training and attend training during duty hours with agency approval. An agency may also reimburse an employee for all or part of the costs of successfully completed training. [5 U.S.C. 4109(a)(2); 5 CFR 410.401]

F. Other Human Resource Management Initiatives

OPM is currently developing human resource management (HRM) initiatives to equip agencies with the flexible systems they need to manage their human resources effectively. The 1998 HRM initiatives are only the beginning of OPM's efforts to improve Federal human resource management; agencies can expect more changes in the future. Some of the 1998 HRM initiatives that may assist agencies in recruiting and retaining IT professionals include--

- Modernizing the current position classification system by establishing a Governmentwide broadbanding authority, with some criteria specified in statute, for current General Schedule positions.
- Providing pay flexibilities and creating more opportunities for using pay to support strategic objectives by--
 - Establishing the flexibility to use the General Schedule as is or, at agency's discretion, create more flexible pay administration features (i.e., pay-setting and within-range pay adjustments), for some or all GS employees, within the basic 15-grade GS salary structure.
 - Enhancing the recruitment and relocation bonus and retention allowance authorities by providing additional payment options (e.g., lump-sum, quarterly, or biweekly payments) and higher payment limits.
 - Increasing incentive award flexibility by establishing an explicit authority for group incentive schemes and raising the limit on cash awards that may be granted without outside approval, but retain Presidential approval of awards above that limit.
- Applying staffing tools to adapt to changing organizational needs by--
 - Maintaining and enhancing decentralized recruiting, examining, and human resource development.
 - Providing hiring and staffing flexibilities, including authorizing categorical rating procedures for selection, establishing a nonpermanent appointment authority, and modernizing the qualifications system by establishing a general qualifications framework.

Additional Recruitment and Retention Incentives

A. Work Life Issues

- Employee Assistance Programs. These programs provide a variety of confidential services, including counseling and referrals, to employees who are experiencing personal problems such as work and family pressures, substance abuse, and financial problems which can adversely affect performance, reliability, and personal health.
- Family Friendly Policies. The Federal Government is a leader in providing family-oriented leave policies and flexitime/telecommuting arrangements.
 - Hours of Work and Scheduling Flexibilities -- provide agencies the discretionary authority to determine the hours of work for their employees. Agencies have the authority to establish:
 - Full-time, part-time, intermittent, and seasonal work schedules;
 - Hours of work for employees, including traditional day shifts, night and weekend duty, rotating shifts, “first-40” schedules, paid and unpaid breaks in the workday (not to exceed one-hour), and overtime; and
 - Alternative work schedules to replace traditional schedules (e.g., 8 hours per day/40 hours per week, with fixed starting and stopping times) with the following:
 - Compressed work schedules (CWS). Compressed work schedules are fixed work schedules that enable full-time employees to complete the basic 80-hour biweekly work requirement in less than 10 workdays.
 - Flexible work schedules (FWS). Flexible work schedules consist of workdays composed of core hours and flexible hours. Core hours are the designated period of the day when all employees must be at work. Flexible hours are the part of the workday when employees may (within limits or “bands”) choose their time of arrival and departure. An agency’s FWS plan may permit employees to earn credit hours.
 - OPM’s Handbook on Alternative Work Schedules provides a framework for Federal agencies to consult in establishing alternative work schedules and information to assist agencies in administering such programs. This handbook can be found on OPM’s web site at www.opm.gov.
 - Telecommuting -- allows employees to work at home or at another approved location away from the regular office.

- Part-Time Employment and Job Sharing -- may help balance an employee's work and family responsibilities.
- Dependent Care Assistance -- is available to help employees with child and elder care needs. Many agencies offer referral assistance to community resources, provide lunch and learn seminars, and sponsor caregiver fairs. Also, OPM issued the *Handbook of Child and Elder Care Resources*, which provides employees, managers, and employee assistance counselors with information about organizations and agencies across the country that can help employees locate quality child and elder care services. Many Federal agencies also provide on-site child development centers.

B. Benefits

- Leave. Sick leave and annual leave policies are generous. Federal employees earn 13 days of sick leave each year. There is no ceiling on the amount of sick leave that may be carried over from year to year. Federal employees also earn 13 days of annual leave during each of their first 3 years of Federal employment. This exceeds the norm of 2 weeks (10 days) in the private sector. Employees earn additional annual leave as their tenure with the Federal Government increases, up to a maximum of 26 days per year after 15 years of service. Most employees can accrue a total of up to 30 days of annual leave for carryover into the next leave year. SES members can accrue up to 90 days of annual leave for carryover. Other leave programs include:
 - Leave Sharing Programs -- allow employees to voluntarily transfer some of their annual leave to specific coworkers or to a leave bank to assist coworkers in dealing with a personal or family medical emergency.
 - Family and Medical Leave Act -- ensures that up to 12 weeks per year of unpaid family and medical leave are available on a gender-neutral basis and mandates job security for employees who take such leave.
 - Other Leave Flexibilities -- sick leave can be used to care for family members, to arrange for or attend funeral services of family members, and for absences relating to adopting a child. Federal employees can receive additional paid leave to serve as bone-marrow or organ donors.
- Health Insurance. Federal employees can enroll in health insurance coverage for themselves and their families at reasonable rates. They enjoy one of the widest selections of plans in the country. Over 350 plans participate in the health insurance program. Employees can choose among managed fee-for-service plans, health maintenance organizations, and point-of-service plans. There is an annual open season during which employees can change their enrollment. Unlike a growing number of private sector health benefits programs, Federal employees can continue their health insurance coverage into retirement with a full Government contribution. Most enrollees pay only one-fourth of the health benefits premium.
- Holidays. Most Federal employees are entitled to 10 paid holidays each year.

- Subsidized Transportation. Agencies can pay for employees' commuting costs to encourage the use of public transportation.
- Pensions. The Federal Employees Retirement System (FERS) is an outstanding 3-tiered plan to provide secure retirement, disability, and survivor benefits for employees and their dependents. In addition to Social Security benefits as a base, FERS offers both an annuity that grows with length of service and a tax deferred savings plan. Employees pay less than 1 percent of salary to qualify for the annuity and are fully vested after 5 years of service and, for disability benefits, after just 18 months.

The savings plan allows employees to save up to 10 percent of salary for retirement. The Government contributes 1 percent of salary to employees who do not contribute and will match up to another 4 percent of savings for employees who do contribute. Because the savings plan is tax deferred, no income tax is due on either the employee's contributions or the Government matching funds, or the earnings on those amounts, until retirement. Employees can choose to invest in any of three funds, or to spread investments across the three funds: a Government securities fund, a bond fund, and a stock fund, all professionally and securely managed by an independent Government agency, the Federal Retirement Thrift Investment Board. A broader selection of investment funds is planned for the near future. Since the inception of FERS in 1987, the performance of this state-of-the-art retirement system has been excellent.

- Life Insurance. Most full-time and part-time employees are automatically enrolled in basic life insurance equal to their salary, rounded to the next \$1,000, plus \$2,000. The Government pays one-third of the cost of this group term insurance. Employees do not have to prove insurability; no physical is required. Basic coverage includes double benefits for accidental death and benefits for loss of limb(s) or eyesight. Employees can also purchase optional insurance at their own expense. Optional coverage includes additional insurance on the employee's life as well as coverage for the employee's spouse and eligible children, if any.

Those younger than 45 receive an additional amount of coverage at no greater cost. The enhancement declines from double the basic amount for those 35 and younger to zero at age 45, when coverage becomes the basic amount.

Accelerated death benefits are available to terminally ill enrollees so that they can receive life insurance proceeds while they are living.

Many large organizations are cutting life insurance benefits to retirees. Untrue in the Federal Government, which allows life insurance to be continued into retirement. It can also be converted to private coverage upon termination, without proof of insurability.

In addition to offering the life insurance program, agencies can pay up to \$10,000 to the personal representatives of employees who die from injuries sustained in the line of duty.

- **Liability Insurance.** A recently enacted law provides Federal agencies with the option of using available funds to reimburse law enforcement officers and managers for up to one-half of the cost of professional liability insurance, protecting them from potential liability and attorneys fees for actions arising out of the conduct of official duties.

C. Resources

- Please contact your local human resources office first for additional information on these recruitment and retention flexibilities.
- Additional information may be obtained from OPM's web site at *<http://www.opm.gov>*.
- The following is a list of OPM program offices that can provide information on these flexibilities:

Employment Service

- Staffing Reinvention Office--Patricia Paige (202) 606-0830

Office of Executive Resources--Joyce Edwards (202) 606-1610

Office of Workforce Relations

- Office of Human Resources Development--Sarah Adams (202) 606-2721
- Work and Family Program Center--Anise Nelson (202) 606-5520

Retirement and Insurance Service

- Retirement Issues--Mary Ellen Wilson (202) 606-0299
- Insurance Issues--Abby Block (202) 606-0004

Workforce Compensation and Performance Service

- Classifications Programs Division--Judy Davis (202) 606-2950
- Performance Management and Incentive Awards Division--
Peggy Higgins (202) 606-2720
- Pay and Leave Administration Division--Jerome Mikowicz (202) 606-2858

Appendix C.

Clinger-Cohen Competencies (IT Functions)

The Clinger-Cohen Act, Section 5002 (3), defines information technology as follows:

“(A) The term "information technology", with respect to an executive agency means equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

“(B) The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

“(C) Notwithstanding subparagraphs (A) and (B), the term "information technology" **does not** include any equipment that is acquired by a Federal contractor incidental to a Federal contract.”

The Clinger-Cohen Core Competencies have been endorsed to serve as a baseline to assist government agencies in complying with Section 5125(C)(3) of the Clinger-Cohen Act. (Revised 9/25/98).

1.0 Policy and Organizational

- 1.1 Department/Agency missions, organization, function, policies, procedures
- 1.2 Governing laws and regulations (e.g., Clinger-Cohen, GPRA, PRA)
- 1.3 Federal government decision-making, policy making process and budget formulation and execution process
- 1.4 Linkages and interrelationships among Agency Heads, COO, CIO, and CFO functions
- 1.5 Intergovernmental programs, policies, and processes
- 1.6 Privacy and security
- 1.7 Information Management (new)

2.0 Leadership/Managerial

- 2.1 Defining roles, skill sets, and responsibilities of Senior IRM Officials, CIO, IRM staff and stakeholders
- 2.2 Methods for building federal IT management and technical staff expertise

- 2.3 Competency testing – standards, certification, and performance assessment
- 2.4 Partnership/team-building techniques
- 2.5 Personnel performance management techniques
- 2.6 Practices which attract and retain qualified IT personnel
- 3.0 Process/Change Management**
 - 3.1 Modeling and simulation tools and methods
 - 3.2 Quality improvement models and methods
 - 3.3 Techniques/models of organizational development and change
 - 3.4 Techniques/models of process management and control models and methods
- 4.0 Information Resources Strategy and Planning**
 - 4.1 IT baseline assessment analysis
 - 4.2 Interdepartmental, interagency IT functional analysis
 - 4.3 IT planning methodologies
 - 4.4 Contingency planning
 - 4.5 Monitoring and evaluation methods and techniques
- 5.0 IT Performance Assessment: Models and Methods**
 - 5.1 GPRA and IT: Measuring the business value of IT
 - 5.2 Monitoring and measuring new system development: When and how to “pull the plug” on systems
 - 5.3 Measuring IT success: practical and impractical approaches
 - 5.4 Processes and tools for creating, administering, and analyzing survey questionnaires
 - 5.5 Techniques for defining and selecting effective performance measures
 - 5.6 Examples of and criteria for performance evaluation
 - 5.7 Managing IT reviews and oversight processes
- 6.0 Project/Program Management**
 - 6.1 Project scope/requirements management
 - 6.2 Project integration management
 - 6.3 Project time/cost/performance management
 - 6.4 Project quality management
 - 6.5 Project risk management
 - 6.6 Project procurement management

7.0 Capital Planning and Investment Assessment

- 7.1 Best practices
- 7.2 Cost benefit, economic, and risk analysis
- 7.3 Risk management models and methods
- 7.4 Weighing benefits of alternative IT investments
- 7.5 Capital investment analysis models and methods
- 7.6 Business case analysis
- 7.7 Integrating performance with mission and budget process
- 7.8 Investment review process
- 7.9 Intergovernmental, Federal, State, and Local projects

8.0 Acquisition

- 8.1 Alternative functional approaches (necessity, government, IT) analysis
- 8.2 Alternative acquisition models
- 8.3 Streamlined acquisition methodologies
- 8.4 Post-award IT contract management models and methods, including past performance evaluation
- 8.5 IT acquisition best practices

9.0 Technical

- 9.1 Information Systems Architectures client/server, collaborative processing, telecommunications
- 9.2 Emerging/Developing technologies
- 9.3 Information delivery technology (internet, intranet, kiosks, etc.)
- 9.4 Security policy, disaster recovery, and business resumption
- 9.5 System life cycle
- 9.6 Software development
- 9.7 Data management

10.0 Desk Top Technology Tools (new)

Appendix D. Information Assurance Functions

All information assurance functions described below include both tactical/deployable systems and strategic or fixed systems. Those that are tied to privileged access are identified as a **CRITICAL FUNCTION** and are shaded.

Function A – IA Certification and Accreditation

- Systems
- People
- Equipment
- Procedures/Policies
- Security

Function B – IA Training/Education

- Professors/Instructors
- Course Developers
- IA Training Administration

Function C – IA Management

- Unit/Base/HQ Levels
- Acquisition of Secure Systems
- Policy/Procedure
- Development
- Implementation
- Compliance
- Enforcement
- Asset Accountability

Function D – System/Network Administration and Operations [critical function]

- Configuration Control
- Installation
- Operations and Maintenance

- System Selection
- Access Control
- Response/Recovery/Reconstitution
- Incident Response
- Operations Monitoring and Analysis
- Countermeasures

Function E – Systems Security Engineering

- Research
- Design
- Development
- IA Planning and Control
- IA Requirements Definition
- IA Design Support
- IA Operations Analysis
- Life Cycle IA Support
- IA Risk Management

Function F – IA Systems/Product Acquisition

- Procurement
- Technical Expertise

Function G – Computer/Network Crime [critical function]

- Forensic Analysis
- Criminal Prosecution/Investigation

Function H – Cryptography

- Operations
- Management

Function I – Threat and Vulnerability Assessment [critical function]

- Red-Teaming
- Penetration Testing
- Threat Analysis

FUNCTION J – COMPUTER EMERGENCY RESPONSE TEAM (CERT) [critical function]

- Clearinghouse for collection of technical vulnerability information

- Clearinghouse for collection of incident reports
- Provide technical expertise to mitigate and reconstitute to victim site following an event/incident
- Disseminate vulnerability information with mitigation solutions (when possible)
- Disseminate threat information
- Coordinate with other CERTs
- Coordinate with appropriate law enforcement agencies
- Coordinate with appropriate counterintelligence agencies

Function K – Web Security [critical function]

- Information management
- Information systems administration
- Information system security

Appendix E. Data Call Results

E.1 Introduction

The IPT developed a data call with the intent to characterize critical aspects of the IA work force. The purpose of this Appendix is to delineate the results of the data call and to explain how the results were derived to provide a context for understanding what the data represent. Overall, the data call was not as complete and systematic as was hoped for, but it did provide significant insights into the IA work force.

The discussion presented here will cover three areas, the approach, the data received (and its limitations), and the insights into the IA work force derived from that data.

E.1.1 Approach

The IPT determined that it wanted the following information about the IA workforce:

- What personnel sources perform IA functions: active military, reserve military, civilians, contractors?
- How is the IA workforce distributed across the IA functions?
- How much of the IA workforce performs IA functions on a full-time basis and how much on a part-time basis?
- What portion of the IA workforce does not consist of IT professionals.
- How much of the IA workforce has received formal training (either computer based or classroom) and how much has received only on-the-job training.

The IPT then developed a survey instrument to collect this information at the unit level. Because of the large size and complexity of DoD a sampling strategy was designed so that the responses to the survey from only selected sites could be used to characterize identifiable segments of the DoD community. The personnel occupation codes that identify personnel as IT professionals are listed in a third section below.

E.1.2 Survey Instruments

The data call survey consists of three instruments in which the participating units characterize their IA work force

- Instrument 1 – a snap-shot of the current IA work force

- Instrument 2 – a judgment about the IA work force currently required
- Instrument 3 – a projection of the IA work force requirements for year 2004

The survey instruments asked the respondents several important questions:

- How many people perform which IA functions in their unit?
- Is IA a full-time or part-time job for these people?
- Have these people received training for the IA functions they perform?
- What categories of personnel are used (e.g., active or reserve military, civilian, contractor)?

In particular, the survey tracks individual persons by the functions performed and the percentage of time performing that function. At the time of the data call, only ten IA functions had been defined. The Web Security function was added as a critical IA function after the data call was completed. Therefore, there is no data on the web security function. The ten functions defined in the survey instruments are listed in Table 5.

Table 5. IA Functions

Function A - IA Certification and Accreditation	Function F - IA Systems/Product Acquisition
Function B - IA Training/Education	Function G - Computer/Network Crime
Function C - IA Management	Function H- Cryptography
Function D - System/Network Administration and Operations	Function I - Threat and Vulnerability Assessment
Function E - Systems Security Engineering	Function J - Computer Emergency Response Teams (CERT)

E.1.3 Sampling Strategy

DoD is a complex organization of 1.4 million active duty military, 0.7 million civilians, and 0.9 million Selected Reserves and National Guard forces. It consists of four Services and over twenty Defense Agencies. The Services alone contain over 40,000 organizational units. Although approximately 90% of DoD reside within the U.S., the remaining personnel are deployed worldwide. Directly querying all of these people and organizations is not a practical way to characterize the IA work force.

Thus, a sampling strategy was adopted. Sampling requires that DoD be partitioned into mutually exclusive and exhaustive subsets, where the IA work force usage is thought to be relatively homogeneous within each subset. Organizational units appear to be a suitable basis for a partition for three reasons:

- Organizational units are identifiable within DoD personnel data, and thus their populations and locations are readily determined
- Organizational units form a mutually exclusive and exhaustive group (i.e., each person is in one and only one unit), and

- Information Technology and Information Assurance services are plausibly related to local area networks associated directly with organizational units

A first estimate is that the partition should be according to three factors,

- Component
- Mission (as indicated by major command affiliation), and
- Size of the organizational element

Once such a partition is defined, the numbers of personnel and the numbers of units in each cell of the partition can be readily determined. By sending the survey to a suitable number of units within each cell the responses can be used to characterize the populations within that cell. Any divergence of the responses within a cell can be used as an indicator that the cells are not sufficiently homogeneous, and additional division may be warranted. If results are missing from a cell or cells, assumptions can be made with regard to how an adjacent cell may characterize the missing cell, and projections would remain feasible, albeit with reduced confidence and accuracy. Component-wide and even DoD-wide results are then obtainable by totaling the projections for each cell in each Component and across all of DoD. Of the elements of the partition, the Service and Defense Agencies are readily identified. Also, major commands or the equivalent can divide each of the Services. The Marine Corps does not have major commands, per se, but the Marine Reporting Unit Code can be used to identify units as combat, acquisition, logistics and so forth. Across DoD the major commands break into the five functional divisions shown in Figure 1.

Unit size is readily available to support a partition of DoD because organizational units are always subsets of individual major commands. Across the 30,000 organizational units in DoD, the median unit size is approximately 270. An analysis of unit sizes in DoD suggests the following breakdown is useful:

- Large units (500 or more people)
- Medium units (100-499 people) (straddles the median; bulk of the population)
- Small units (10-99 people)
- Tiny units (less than 10 people) (most are in shared locations; special case where tiny units are solitary (Tiny-s))

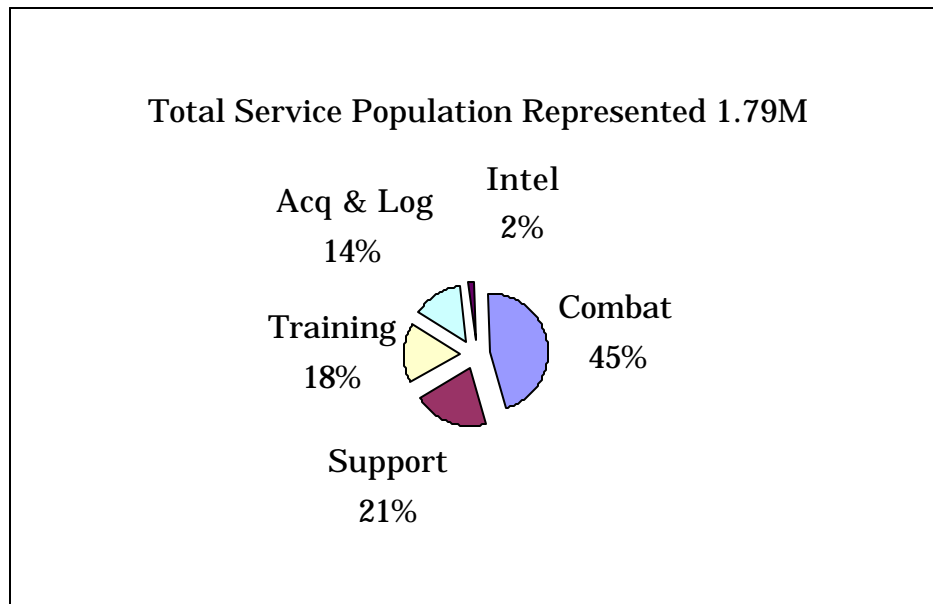


Figure 1. Total Service Population Divided by Type of Major Command

The partition by Service and major command function is significant because experience has shown that Service procedures frequently vary along those lines. However, the effect of unit size on IA usage appears to be more intuitively obvious. Large units are expected to employ full time, professional system administrators and related positions, and they are expected to service a relatively large user base. On the other hand, small units are expected to require larger numbers of part time IA positions, working less intensively on an individual basis and serving a relatively limited user base.

These slices across DoD partition it into the framework shown in Figure 2. The multiple pages for each case is intended to show multiple Services, broken down on the basis of function and unit size. A “case” is a single cell in this figure, and it corresponds to a choice of a single Service, a single function, and a single size of unit.

When the cells for each of these cases were examined to determine the numbers of units and the populations of each, it became clear that not all of the cases were of equal significance, nor were an equal number of samples needed for each. For the large units, the numbers of units in any one function could be limited, and in many cases one or two samples appeared to be reasonable for the case. In other cases the numbers of units were small enough for some functions that the cells were combined to make viable groups. The resulting numbers of cells and samples for the Services are summarized in Figure 3.

Several additional cases were considered beyond the Service infrastructures. The Navy and Marine Corps each had significant numbers of tactical forces, either assigned to ships, or assigned to tactical units that were stationed on ships. These were treated as a separate case from the Service infrastructures.

The Defense Agencies each fell into a single one of the functional categories, and they were treated separately. Units were somewhat more problematic for the Agencies, with no centralized lists of unit names and addresses maintained by the Defense Manpower Data Center, as had been the case for the Services. However, the combination of Component and

geographic location appeared to be a viable surrogate for the agencies. The overall sampling plan for the IA requirements is summarized in Table 6.

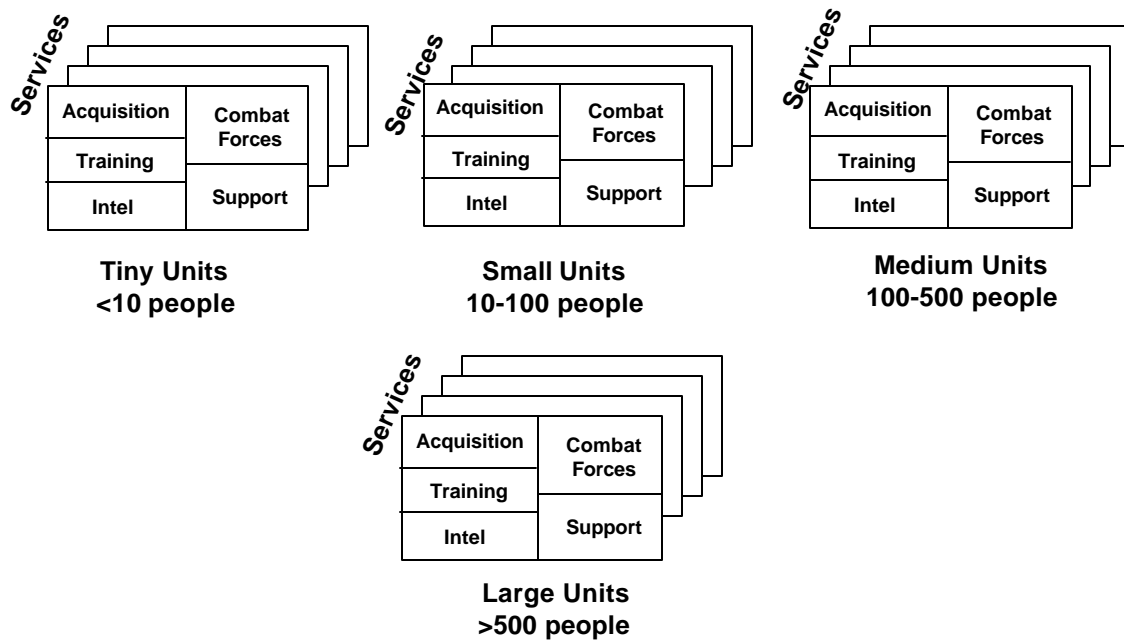


Figure 2. Framework for IA Results

Framework for IA Requirements					
Function Acquisition/ Logistics Size	Intelligence	Combat Forces	Support	Training	
Large ([≥] 500 ppl)	<div>Army Units 18 Cases, 405 Samples</div> <div>Navy Units 27 Cases, 280 Samples</div> <div>Marine Corp Units 14 Cases, 95 Samples</div> <div>Air Force Units 19 Cases, 350 Samples</div>				
Medium (100-499 ppl)					
Small (10-99 ppl)					
Tiny (<10 ppl)					
Tiny-Solitary (<10, alone)					
Total for the Services: 78 cases, 1,130 samples					

Figure 3. Summary of Service Infrastructure in IA Sampling Requirements

Table 6. Sampling Plan for IA Data Call

		Cases	Samples
Services	Infrastructure	68	1,050
	Afloat/Tactical	10	80
Agencies		17+	65+
Grand Total for Survey		95+	1, 195+

The Services and Agencies were provided the details of this sampling plan to aid their collection of data and to help ensure an adequate number of samples and cases would be returned to make the analysis feasible and meaningful.

E.1.4 Identification of IT Professionals Within the IA Workforce

One of the objectives of the data call was to determine whether the IA work force consists mostly of IT professionals, or personnel from other specialty areas assigned IA duties on a collateral basis. Thus, for each individual identified as performing an IA function, the military occupational specialty code or designator was requested. Those personnel with specialty codes listed in Table 7 were considered IT professionals.

Table 7. IT Occupational Codes Within DoD

Type	Occupation Code	Title
<i>Army IT Specialists</i>		
Enlisted	74B	Information Systems Operator-Analyst
Enlisted	74C	Record Telecommunications Operator-Maintainer
Enlisted	74G	Telecommunications Computer Operator-Maintainer
Enlisted	74Z	Information Systems
Officer	25A	Signal, General
Officer	53A	Systems Automation Management
Warrant	250N	Network Management Technician
Warrant	251A	Data Processing Technician
<i>Navy IT Specialists</i>		
Enlisted	RM	Radiomen
Enlisted	NEC2735	Information Systems Administrator
Enlisted	NEC2779	Information Systems Security Manager
Enlisted	NEC2780	Network Security Vulnerability Technician
Enlisted	NEC27871	Advanced Network Analyst

Type	Occupation Code	Title
LDO	6420	Automated Data Processing
Warrant	7420	Automated Data Processing
Officer	0045	(Secondary MOS) Command and Control
Officer	0046	(Secondary MOS) Information Warfare
Officer	0055	(Secondary MOS) Electronic Engineering
Officer	0076	(Secondary MOS) Space Systems Operations
Officer	0077	(Secondary MOS) Space Systems Engineering
Officer	0089	(Secondary MOS) Information Technology Management
Officer	0091	(Secondary MOS) Information Technology Science
<i>Marine Corps IT Specialists</i>		
Enlisted	4066	Small Computer Systems Specialist
Officer	0602	Communications Information Systems Officer
<i>Air Force IT Specialists</i>		
Enlisted	3A0 Series	Information Management
Enlisted	3C0 Series	Communications-Computer Systems
Enlisted	3C1 Series	Radio Communication Systems
Enlisted	3C2 Series	Communications-Computer Systems Control
Enlisted	3C3 Series	Communications-Computer Systems Planning and Implementation
Officer	33S Series	Communications and Information
<i>Civilian IT Specialists</i>		
GS	0332	Computer Operation
GS	0334	Computer Specialist
GS	0335	Computer Clerk and Assistant Series

E.2 Data Received

A summary of data received for analysis is shown in Table 8. The table lists all of the Services and Agencies participating in the data call, and two sets of columns, one for the data requested, and one for the data received. Within each set of columns, the reference to cases represents the number of cases analogous to the cells in Figure 2, and the reference to

samples indicated the total number of units to be queried—roughly 10 to 30 samples per case in the initial data call design.

Table 8. Data Call Response Received⁴

	Data Requested		Data Received	
	Cases	Samples	Cases	Samples
Army	18	405	16	50
Navy	27	280	21	25
Air Force	19	350	11	59
Marine Corps	14	95	5	11
BMDO	1	1	Entire agency	
DIA	1	1	1	1
DISA	3	25	*	15
DLA	5	45	*	36
DoD IG	3	16	Entire agency	
Joint Staff	Did not specify		*	18
NIMA	1	1	Entire agency	
NSA	1	1	Incomplete	
WHS	1	5	1	5

The Services, listed in the top section of the table made some effort to follow the sampling strategy outlined above. Because the Services contain the great majority of DoD personnel and IT systems, their results are central to this data call.

The Agencies generally did not use the sampling strategy because the local definitions of unit identification code were either unavailable for the effort or the Agencies chose not to use them. In some cases Agencies did a full survey, and in other cases, they developed alternative sampling strategies. The intelligence agencies (DIA, NSA and NIMA) carried out their own surveys and provided limited results for the study. The results from the DoD IG showed that the IA usage pattern was entirely different⁵ from the rest of DoD, and therefore their results were not combined with the other organizations. Results from the Agencies covered through this effort are discussed below when and where results could be made available in a form similar to the Service data analyzed.

⁴ Data received did not fit the proposed sampling structure.

⁵ The DoD IG reported approximately 30 work years involved in professional investigations of computer intrusions, and 0.6 work years in system administration for the entire agency. All other DoD organizations showed significant usage of most IA functions and primary system administration, but practically no investigation of computer intrusions. Thus, the DoD IG results were essentially disjoint from the other data.

The response of the Services to the data call was at best incomplete, and this significantly reduced the confidence that can be placed in the results of the effort. Two kinds of problems are evident in Table 8:

- Service data failed to cover many of the cases requested, except perhaps for the Army, which did cover 16 of 18 cases identified in the sampling framework. Other Services data failed to cover a significant fraction of the cases in the framework: 22 percent (Navy), 42 percent (Air Force) and 64 percent (Marine Corps) of the cases in the framework. These cases were identified in the Framework because IA usage was presumed to differ for each case, and the lack of coverage means that significant fractions of each Service are not sampled and are being represented by an average based on the samples that were taken.
- Whereas the initial plan called for 10 to 20 cases per sample, the actual data reflects between 1 and 5 cases for sample, depending on the Service. Such low sampling rates increase the chance that atypical units may be projected to represent some cases. Thus the simple statistical reliability of the data call is minimal.

The main problem with the low response rates shown in Table 3 is the potential they raise for flawed (non-representative) data collection. The uncontrolled potential for bias because of the low reporting rates appears to be the primary source of error in the sampling, even though the statistical reliability of the data is also marginal at best. Uncontrolled biases could be manifested in several ways:

- Units with minimal investment in IA may be more likely to respond than units with more significant IA investment because the reports are easier to do—there is less to report. This effect would tend to understate the actual DoD IA usage.
- Units engaged in a local IA debate might be more likely to respond to the data call if they view it as a means of furthering one side of the debate. This could affect the accounting, but the bias could either overstate or understate DoD IA usage.

The objective of the analysis was to use the data from the data call, despite its limitations, to make the best representation of IA usage across all of DoD. In defining the sample cases (Figure 3), it was realized that some cases covered relatively small portions of DoD, whereas other cases covered relatively large numbers of people. Thus we needed to weight the results for each case in an appropriate manner so that samples representative of large populations are weighted more than those that are representative of small populations. A personnel database, covering all DoD active military and direct hire civilians was used to establish both the framework and the weightings appropriate for each case in the framework.

The analysis for each case in the framework used the simple assumption that all of the units in each case had the same ratio of IA counts (e.g., for people, work years) to unit population as did the units that were sampled in the data call for that case. Since the population of each case is known from the DoD personnel database, the IA totals follow directly from the assumption.

A complication arises for the cases for which no samples were provided. In those cases, the ratio of the IA counts to the population that was sampled was used to characterize the population that was not sampled. This assumption is likely to introduce error, but no

practical alternatives are evident. Table 9 summarizes the scaling that was used in this process. For the cases where data were available, two percent (32,885/1,538,313) of the covered population were actually sampled. The covered cases are then, in effect, scaled up by another 30 percent (2 million/1.5 million) to cover the portion of DoD in the cases for which the Services provided no data.

In the counts of IA personnel and resources provided by the Services, approximately 10 percent of the work were actually provided by reserves or contract personnel. Neither contractors nor reserves were included in the personnel counts used to scale the results. Because of the methodology used (described above), the total counts of IA work years or IA personnel would remain valid as projections of DoD usage of IA. However, including contractors and reservists could lead to an overstatement of IA as a *fraction* of the total Service-generated work years, by approximately 10 percent, because contractors and reserves were not included in the figure for total Service work years.

Table 9. Population Count Used to Scale the Services

Service	Personnel Counts			
	IA Personnel Reported in Data Call	Total Personnel from Units Reporting in Data Call	Total Personnel in Cases with Data Available	Total Personnel in Service (Military + Civilian)
Army	779	14,087	653,925	711,299
Navy	326	7,901	384,587	568,100
Air Force	596	7,106	435,000	543,047
Marine Corps	248	4,189	64,801	183,659
Total	1,949	33,283	1,538,313	2,006,105

E.3 Results

As a result of the data call, insights were developed into four areas of DoD IA usage:

- Resources by IA function
- Part time vs. full time IA support
- Training background for IA personnel
- Types of personnel providing IA support

E.3.1 Resources by IA Function

The first topic of interest in DoD IA is the resource distribution in IA functions. In Figure 4, the resource distribution for Services IA work years over the ten functions defined in the original survey is displayed as percentages of the total work years generated by each Service. Despite the limitations in the data, a pattern clearly emerges that is similar across the Services.

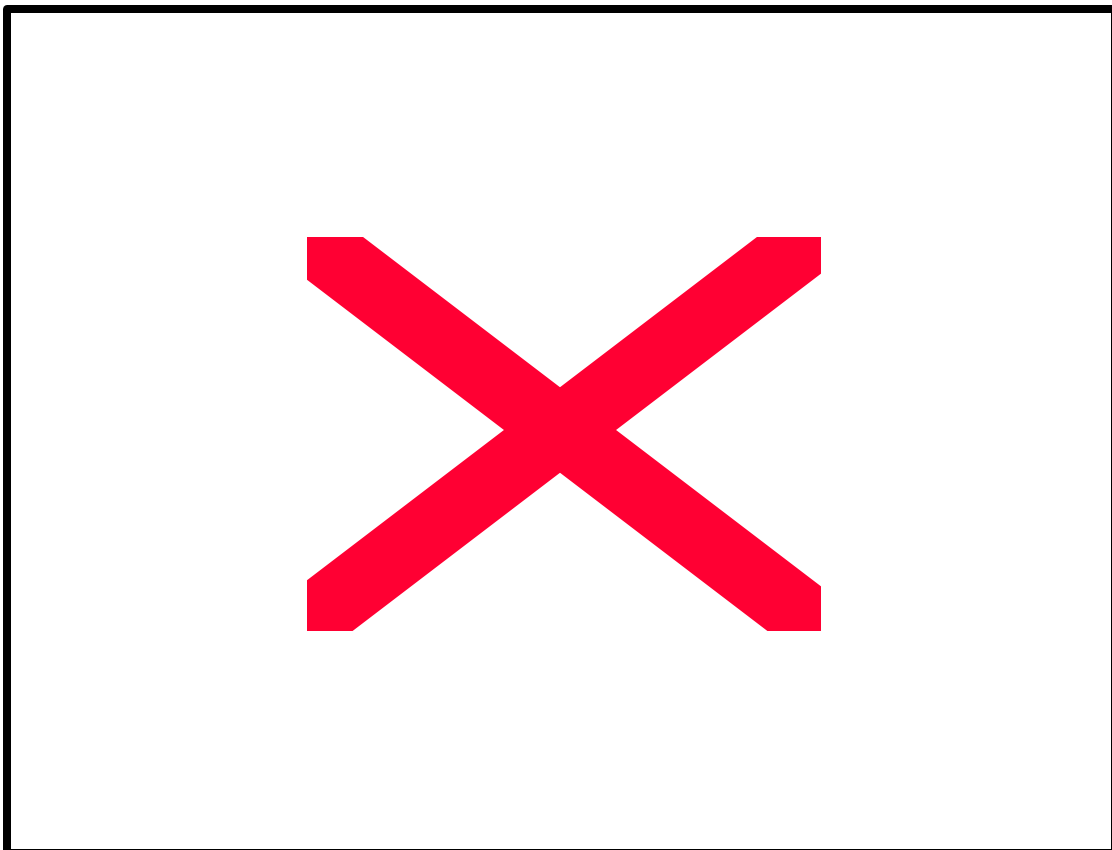


Figure 4. IA Resource Distribution by Function for the Services

For each Service, System/Network Administration dominates the list of functions and generally accounts for about half of the total effort:

- The Air Force, with 3.7% of its total manpower in System/Network Administration, has the largest per capita system administrators. This is equivalent to having approximately one system administrator for every 27 people. Several limitations discussed above (Section 2) could overstate the Air Force usage of IA based on this data.
- The Army is next with 3.5%, which translates to approximately one system administrator for every 30 people.
- The Marine Corps has the next highest System/Network Administration usage at 3% (one system administrator for every 34 people). The Marine Corps data suffer from low response rate to the data call, resulting in unreliable scaling.
- The Navy has the lowest IA resource of the Services. Only 2% of Navy's total manpower is in System/Network Administration. Therefore, there is one system administrator for every 50 people. The Navy also had very low data response rate, with attendant unreliable scaling.

Of the original ten IA functions, four are defined as critical: System/Network Administration and Operations; Computer/Network Crime; Threat and Vulnerability Assessment; and Computer Emergency Response Team (CERT).

Table 10 summarizes the results for Service IA resources. The first two columns indicate the total work year resources associated with IA, and the fraction of all Service-generated work years that they represent. The last two columns show critical functions resources as a percentage of the Service total IA resources. System/Network Administration takes up roughly half of the total IA resource. The other critical IA functions use only a small fraction of the total IA resource.

Table 10. Summary of IA Service Resources

Service	Total IA Work-Years	% of Total Service Work-Years	Critical IA (% of Total IA)	
			System/Network Admin & Ops.	Other Critical IA
Army	48k	6.8%	51%	1%
Navy	24k	4.2%	48%	1%
Air Force	38k	7.0%	54%	5%
Marine Corps	8k	4.5%	64%	1%

The Agencies typically show the same type of distribution as the Services for IA functions except for Agencies with specialized missions. These special cases—DIA, NIMA, DISA, and DoD IG—are presented below. DIA and NIMA are both intelligence agencies, and show System/Network Administration as the dominant IA usage in Figure 5 and Figure 6. Fully 91% of the IA at DIA is for System/Network Administration, and 73% for NIMA.

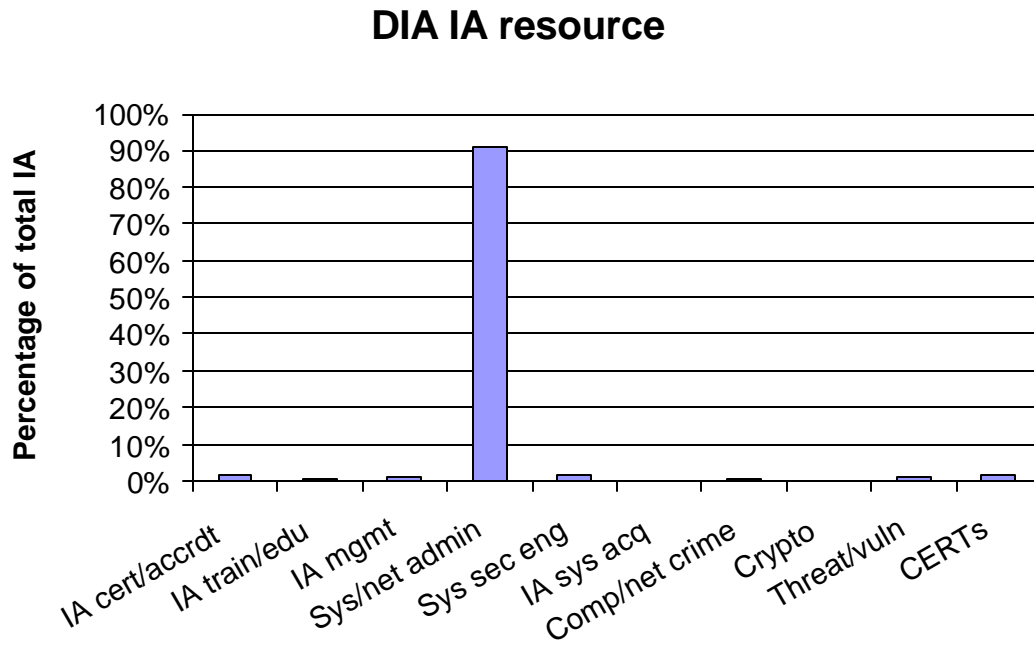


Figure 5. Relative Distribution of DIA IA Resource by Function

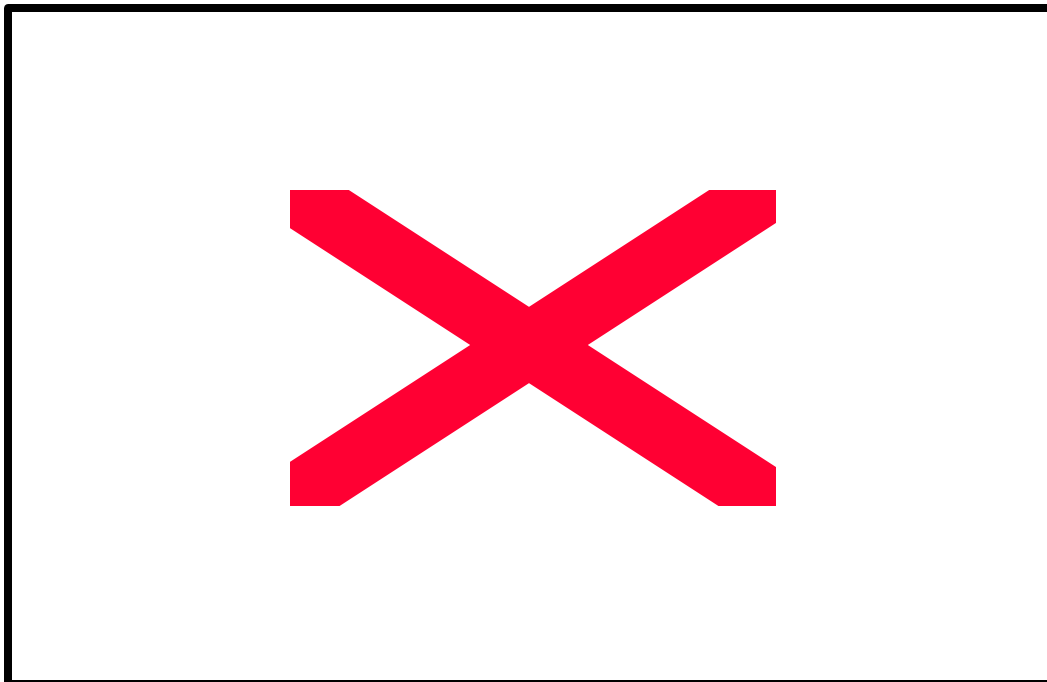
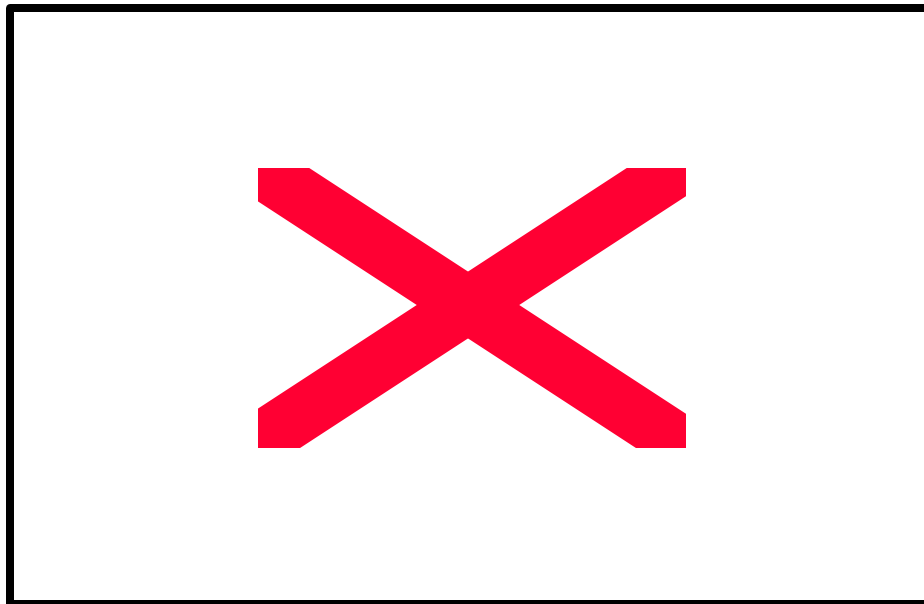


Figure 6. Relative Distribution of NIMA IA Resources by Function

DISA total is shown in Figure 7. DISA is a case where the UICs maintained by DMDC do not reflect the DISA organization, but the DISA Organization & Manpower Division, provided an alternative approach. In particular, some of the DISA units actually provide IA service for other groups within DISA. The total number of personnel within the organizations served by the sampled units is 2,917. These IA personnel are applied against the whole DISA customer base in determining the ratio of IA to total people. DISA's IA usage remains very high at approximately 14 percent (compared to 4 to 7 percent for the Services). The difference in the distribution of IA resources can be expected to be due to the specialized mission of DISA. DISA WESTHEM did not submit any samples in the data call, and the results might have been different if WESTHEM were included.

DoD IG is also a specialized case because of its criminal investigative nature. DoD IG addresses Computer/Network Crimes almost exclusively. GS-1811 professional criminal investigators do all investigations. Because the data are so disjoint, the DoD IG data are not aggregated with other data in this report.

Figure 7. Reported DISA IA Resources by Function



E.3.2 Part-Time vs. Full-Time IA Support

Another topic of interest is the distribution of full-time and part-time IA personnel. More full-timers may promote efficiency and possibly reduce training and certification pipe lines. Figure 8 shows the break down of the IA personnel for the Services by 10% intervals of the amount of time spent on IA. The scale is chosen to have a maximum of 40,000 people for Army, Navy, and Air Force to aid in comparison between Services.

- The Marine Corps is plotted on a smaller scale simply due to its smaller size.
- With the exception of the Navy, the Services have more than half of their IA workers doing at least 75% time on IA. The Navy however, has its people spread throughout the spectrum.

- Some of the Agencies have similar distribution as Army, Air Force and Marine Corps. A plot showing their distribution is shown in Figure 9.

Some of the other Agencies have peculiar distribution of full-time vs. part-time IA workers compared with the other groups already covered. The results for these Agencies are plotted in Figure 9.

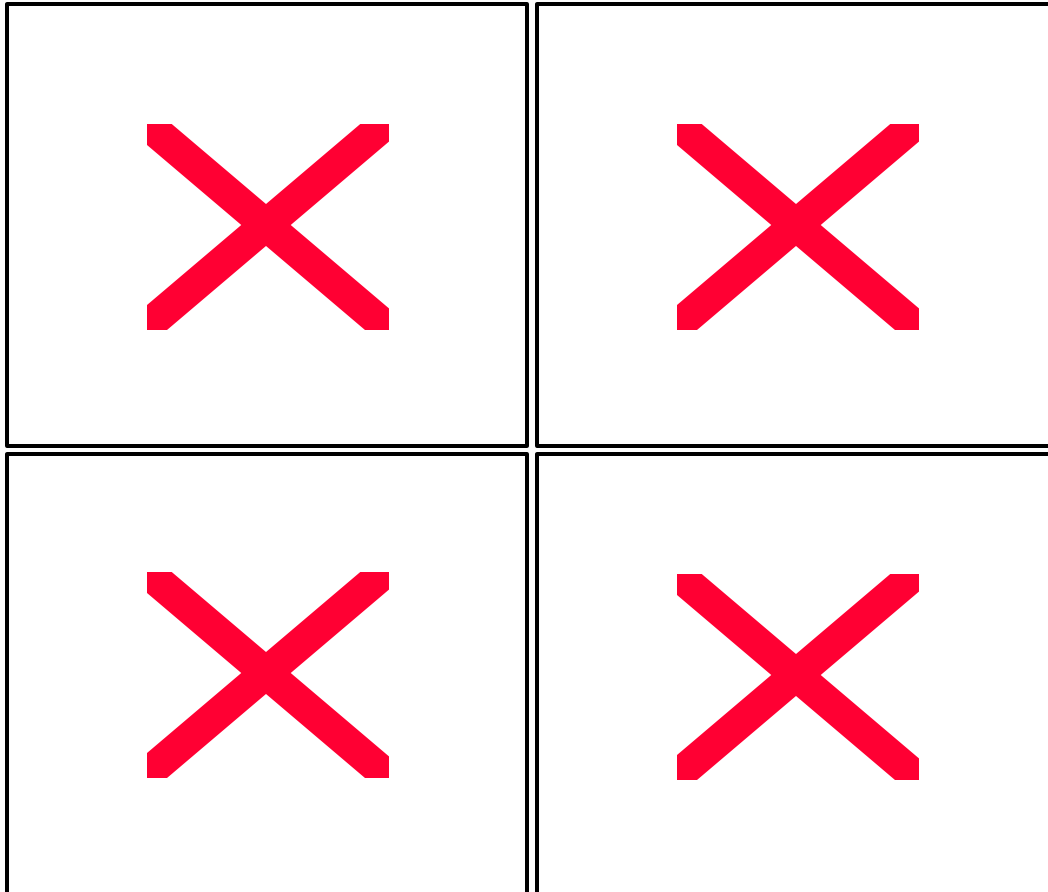


Figure 8. Personnel vs. Time Spent on IA for the Services

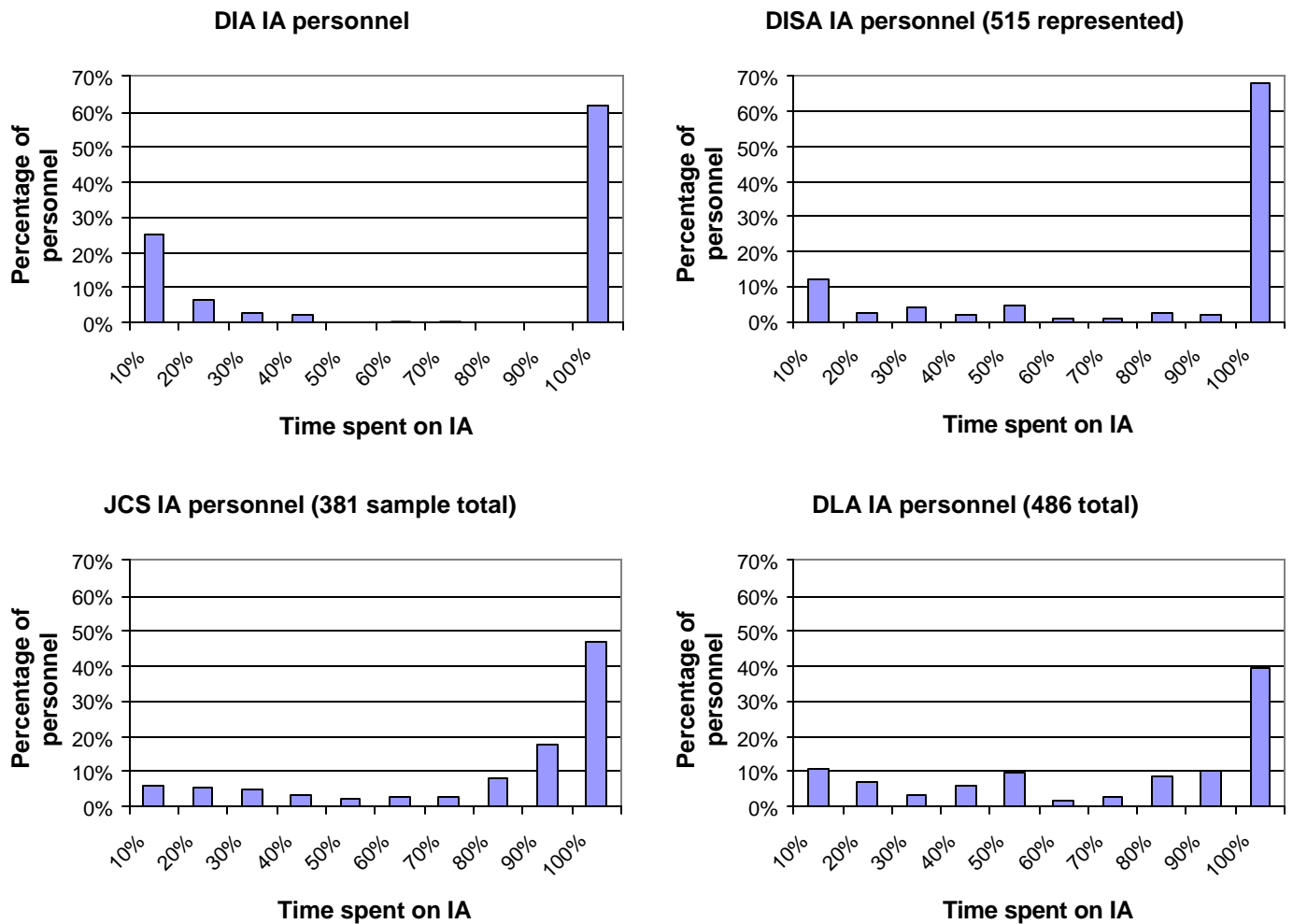


Figure 9. Full-Time vs. Part-Time Distribution for DIA, DISA, JCS, and DLA

E.3.3 Training Background for IA Personnel

The final two topics covered in this analysis address training issues. The first part, training background, addresses whether the IA worker has had formal training for the IA function to which he or she is assigned. A person is considered to have had formal training if he or she has gone through either class room training or computer based training (CBT). Contractors are assumed to be formally trained if the IA function they perform is specified in the contract.

A distinction should be drawn between someone who is performing a critical function, defined in Section 3.1, as opposed to someone who is not. It is much more important that the person doing a critical IA function be properly trained. For the plots presented here, the

raw responses, rather than case-weighted results, will be used to facilitate comparison among Components. Figure 10 shows the level of training for the Services.

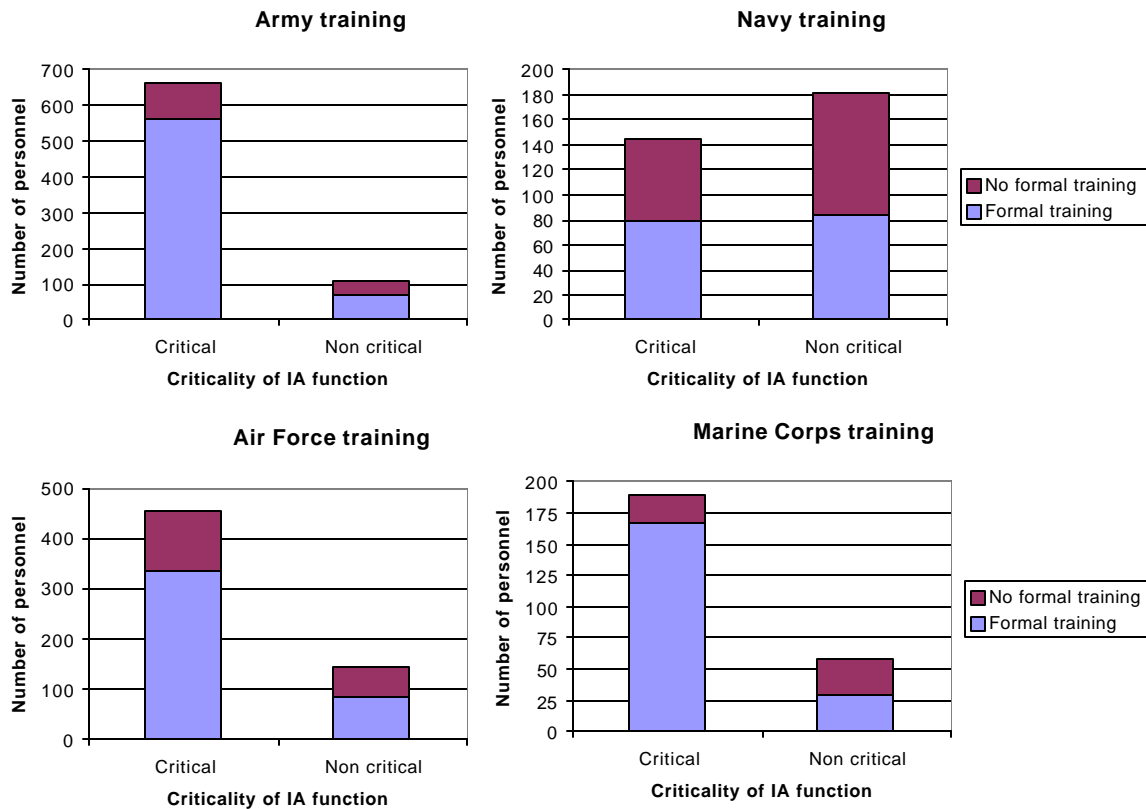


Figure 10. Level of Training for the Services

Some observations based on Figure 10 include:

- Training has been provided to ~80% of the IA workforce (not including Navy)
- Personnel with critical IA functions out-number personnel without critical IA functions by roughly 4 to 1 (again, not including Navy)

The data appear to show the Navy with fewer people trained than the other Services, and a much lower usage ratio of critical to non-critical functions. It must be emphasized again that the Navy data call response rate is very low, and the data may simply be invalid with regard to these issues. The Navy training statistics may, however, be linked to the use of part time personnel for critical functions. Figure 10 shows that the Navy uses part time personnel to a greater extent than the other Services. The low level of training indicated here does warrant further examination.

The level of training for the Agencies appears to be similar to that of the Services. Table 11 shows a summary of level of training for the Agencies by the percentage trained. The data for DIA was not included because the training field was not completed consistently for the personnel identified on the DIA data call.

Table 11. Level of Training for the Agencies

	Percentage Trained	
	Critical IA	Non critical IA
BMDO	94%	13%
DISA	87%	96%
DLA	64%	78%
DoD IG	91%	None
Joint Staff	75%	64%
NIMA	99%	0%
WHS	81%	70%

E.3.4 Types of Personnel Providing IA Support

The question of personnel background is harder to track. One of the problems stems from the way the data call instrument was crafted. The respondents were asked to report the Occupational Code for the IA personnel identified. This resulted in inconsistent answers due to the different interpretation of the question being asked. The Army and the Air Force had the best and most consistent response to the question of occupational series, whereas the Navy and the Marine Corps responses did not provide usable data. Better response may have been possible had the desired Occupational Codes for IT professionals been identified a priori and given to the survey respondents to choose.

The organizations in the Services and Agencies with data that supported a personnel background breakdown are shown in Figure 11 and Figure 12. Four categories of personnel types are considered here:

- Contractors (can be considered most likely to be IT professionals)
- IT Professionals (personnel identified by their Occupational Codes)
- Other Specialists (all other Occupational Codes)
- Unspecified (no Occupational Code provided).

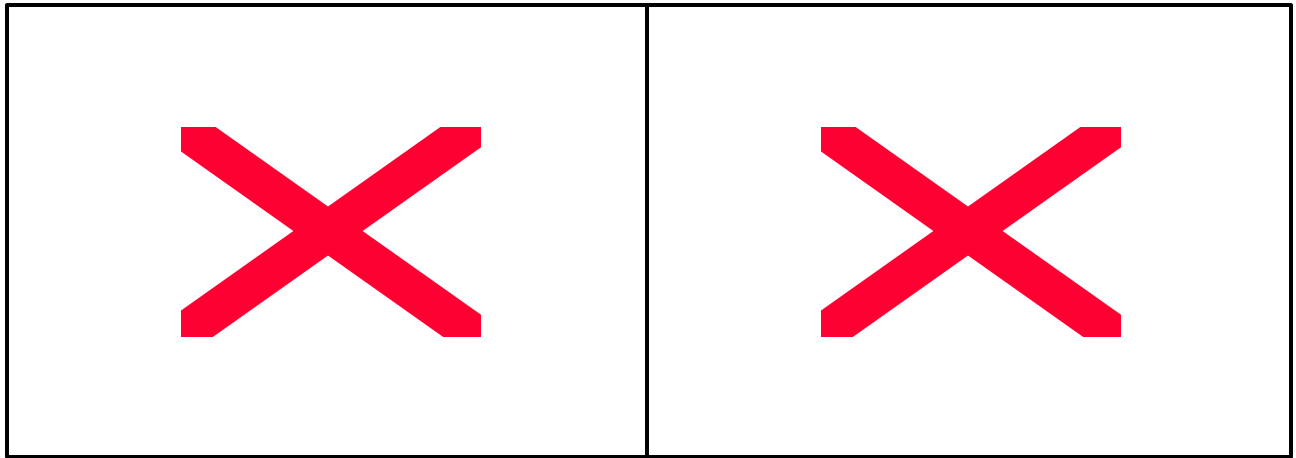


Figure 11. Personnel Background Breakdown for Army and Air Force

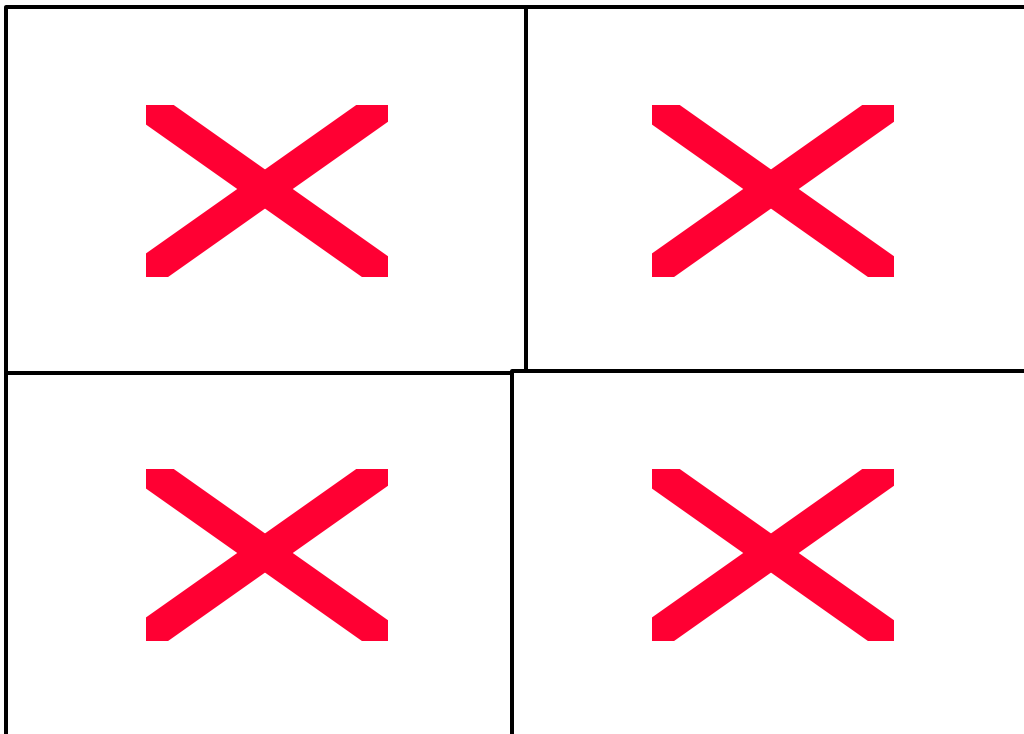


Figure 12. Personnel Background for Selected DoD Agencies

Appendix F. Military IT Occupational Specialties

Background

General

The military personnel subgroup of the IPT reviewed the personnel management of those personnel who perform IT/IA functions. The initial goal was to use the results of the data call to see what personnel policies, practices, etc., should be established in the Department. The subgroup was not able to fulfill that goal due to the lack of timeliness of the required data. Therefore, it focused its efforts on management of *established military IT occupational specialties* in each Service. Though the term “information technology” is defined, who is an IT professional is widely interpreted. Therefore, the occupational specialties discussed in this appendix represent those that the Services consider to be their IT occupational specialists.

Career Fields

Each of the Services has established IT occupational specialties for both officers and enlisted personnel who are managed by career field managers. The Army, Air Force, and Marine Corps are specialized to the extent that their professional personnel serve tours primarily in their career fields and have established career tracks. Career progression allow both officers and enlisted to progress from junior enlisted and officer ranks to the E -8/9 level for enlisted and O-6/7 level for officers. In some cases, merging of skill ratings or specialties at upper pay grades has been accomplished to allow for continued progression.

The Navy manages its professional IT officer force through a subspecialty system. Officers in other career fields receive training and/or experience in IT fields before becoming subspecialists. Ideally, they alternate tours between their primary specialty and their subspecialty fields, but compete for promotion in their primary occupational field. The Navy’s management of its enlisted IT professionals is similar. The Navy identifies its personnel through an NEC system with Radioman the primary rating in the IT skill areas. However, other occupational specialties such as Cryptologic Technician (CT) and Firecontrol Technician (FT) may source into IA/IT NECs. Unlike officers, enlisted personnel with IT NECs can normally expect to be assigned by their NEC specialty. Competition for promotion, however, is done against the parent rating.

Retention

Retention of experienced IT military personnel is a concern for each of the Services. In the last three years, an increase in the number of experienced IT personnel leaving the military

has been documented. Reasons cited include PERSTEMPO/OPTEMPO, private sector opportunities, retirement benefits, and career progression (in some cases).

Each of the Services has recognized the difficulties in retaining experienced personnel, and has taken a number of actions to boost retention to retain experienced personnel and meet end-strength requirements. These actions include:

- **Selective Reenlistment Bonuses (SRB).** Each of the Services is using SRB to retain enlisted personnel. The overall trend in the last three years has been to increase the multiple offered. Increasingly, the Services are offering SRB to second term personnel (6 to 10 years of service) and careerists (10 to 14 years of service). The effectiveness of retaining personnel using SRB has varied by Service. The Army and Navy have reported favorable “take rates,” while the Air Force and Marine Corps are more guarded in their assessments of its effectiveness.

SRB is budgeted annually in the POM for each of the Services. Each of the Services manages a master SRB budget, and money is allocated subject to Service priorities. Because retention is an issue throughout DoD, the amount of money allocated to SRB within DoD has increased significantly in the last three years.

While there is a reenlistment bonus for enlisted personnel, there is not an equivalent for officers in the IT workforce.

- **Education.** Each of the Services is using advanced education to assist in retaining personnel. The Services allow personnel to obtain a fully funded degree in return for a service obligation. It should be noted, however, that educational programs are most often completed during a service member’s “off duty” time, and can be difficult to start and/or successfully complete given service commitments such as deployment.
- **Commercial certification.** The Navy, Air Force, and Marine Corps are looking closely at allowing personnel to participate in commercial certification programs. In return for receiving commercial certification from companies such as Microsoft, personnel agree to reenlist or extend their contracts. The Navy is expecting to train 2,000 Microsoft Certified Systems Engineers per year starting in FY 99. The Air Force is currently working a similar pilot program that will begin in FY 00. In FY 01, they will assess the effectiveness to determine if the program should be used Air Force wide. The Marine Corps has initiated a program, but is still assessing whether the program is going to be successful in retaining personnel.
- **Lateral conversions.** Each of the Services is allowing personnel in other career fields, particularly those that are being disestablished or are over-manned, to laterally convert into IT specialties if they meet the skill requirements. This program has been generally successful in each of the Services.
- **Prior service personnel.** Each of the Services is allowing personnel who have left the Service to return if they meet certain guidelines. However, relatively few personnel are being recruited/retained in this manner.
- **Continuation beyond separation gates.** Each of the Services is accepting and approving, on a case-by-case basis, requests for personnel who are non-selected for

promotion but are approaching high year tenure gates to stay in the Service for specific periods of time.

- **Steering Groups.** Beyond the use of career field managers, the Air Force recently established an officer steering group composed of senior personnel from the IT communities to review the management of their officer/enlisted/civilian IT career fields. Though not a new approach, the group made positive recommendations to the management of the officer corps that have been adopted by the Service. The Navy has also used the same approach. It has established an Executive Steering Group to oversee the career IT training of all Department of the Navy personnel as part of its Computers, Information Systems, and Networks (CISN) strategy.

Accessions

Each of the Services uses computer models to assist in determining the appropriate number of personnel to recruit for IT career fields. While personnel with the prerequisite ability to become IT occupational specialists are actively sought, the Services' goal is to recruit personnel for the Service first. Once recruited, uncommitted personnel undergo aptitude/physical screening before being classified for an IT occupational specialty or other positions. Enlistment incentives (e.g., bonuses, college funds) are used in varying degrees by the Services (Navy and Air Force) to attract personnel into IT occupational specialties.

The working group reviewed the accession goals versus actual accessions for each of the Services for the last three years:

- The Army, Navy, and Marine Corps each reported that they met their accession goals for IT officers and enlisted personnel for FYs 96 through 98.
- The Air Force reported that it met its goals for accessing personnel for enlisted IT occupational specialties for the same time frame. The Air Force, however, has not been able to access enough IT officers. The Air Force requirement to sustain the IT officer career field has been 414 personnel but has fallen short of that goal in each of the last three years (FY 96 – 340; FY 97 – 300; FY 98 – 285). In addition, 436 IT personnel retired or separated from the Air Force during the same period. The Service is reporting that it is currently on target to meet its accession goal for officers in FY 99, and is projecting to recruit 390 personnel in FY 00.
- Each of the other Services reported that it is on track to meet its accession goals for officer and enlisted IT occupational specialties for FY 99.

The use of waivers to meet accession goals was also reviewed. Each of the Services reported that it used waivers, that waivers assist in meeting goals, but that waivers were given only when other information identified that applicant as having good potential.

In those cases where retention efforts do not appear to be adequate enough to meet projected end-strength requirements, the Services have increased the number of personnel recruited. In some cases, that number has been increased beyond the number of billets authorized for the lower paygrades. This approach ensures not only that there are adequate numbers of personnel to meet end-strength requirements, but also provides a larger cohort

to retain from. The ability of the Services to expand training capacity for additional personnel may become a limiting factor.

Although none of the Services has specific policies, programs or advertising campaigns to recruit IT occupational specialists, some initiatives are being reviewed and/or pursued by the Services. The Navy recently instituted a Tech Prep program. In this program, students attend a community college for six to twelve months, followed by training in the Navy. College credit is earned in the Navy's school pipeline. Ultimately, personnel earn an associate's degree, and the Navy gains an already trained enlistee. Along the same line, developing an internship type program where students can gain experience in IT career fields during summers and other school vacations is an idea under review.

The Navy has revamped curricula for IT at the Naval Postgraduate School and the Naval Academy. The Air Force has done the same at the Air Force Academy and the Air Force Institute of Technology. In addition, the Air Force is changing the training curriculum for its enlisted personnel in IT specialties to focus more on networking and IA.

Focusing ROTC dollars toward IT curricula is an idea that was also reviewed. The concept is to target ROTC scholarships to undergraduate IT degrees. The Air Force already allows up to 13% of its ROTC scholarships to be offered for computer science and computer engineering degrees. However, personnel may still select other Service career fields at graduation such as aviation. The Services want a more experienced workforce at commencement of military service.

Allowing personnel to enter the military through a lateral entry program similar to that currently in place for health care professionals was also reviewed but bears further analysis prior to being pursued. The idea has merit because it would provide an option to recruit experienced personnel from the civilian sector, but other considerations, such as a reasonable expectation that the program would succeed, necessitate additional study.

Air Force

Enlisted

The Air Force has several established and closely managed enlisted career fields that allow adequate career progression in the enlisted ranks. In the last three years, the Air Force has observed a decline in retention in many of the IT specific enlisted career fields, with PERSTEMPO and private sector opportunities cited as the primary reasons. With a goal of retaining 55% of its first term personnel, 75% of the second term personnel, and 95% of the career personnel, the Air Force has implemented various programs to improve retention of experienced personnel and meet end-strength requirements. These include (1) increasing SRB for first- and second-term personnel, and providing a first-ever SRB for careerists; (2) using commercial certification as a reenlistment tool; and (3) allowing personnel with prior service to return to active duty. Additional manpower is needed to meet the challenge of the proliferation of networks and databases, and Air Force career field managers are pursuing authorization to conduct a manpower study to document the requirement. Additional manpower should assist in reducing PERSTEMPO.

To meet end-strength requirements, the Air Force has increased the numbers of personnel being accessed, and, and is using enlistment bonuses for four- and six-year first term enlistees.

The following tables provide retention rates by terms of enlistment by career field:

Table 12. Information Management (3A)

Year	Skill	1 st Term %	2 nd Term %	Career %	Billets	Inventory	SRB
FY 96	3A	80	80	96	12,700	13,500	0/0/0
FY 97	3A	60	75	95	12,000	12,700	0/0/0
FY 98	3A	66	73	93	11,732	12,236	0/0/0
FY 99*	3A	69	66	90	11,400	12,100	0/0/0

*FY99Q1

Remarks: Information managers are currently being trained as workgroup managers (they work at the unit level to assist personnel with computer applications, minor PC repairs, etc.). No SRB is offered; however, the current retention trend is being monitored closely.

Table 13. Communications/Computer Systems Operator (3C)

Year	Skill	1 st Term %	2 nd Term %	Career %	Billets	Inventory
FY 96	3C	61	68	91	N/A	15,556
FY 97	3C	52	62	91	14,886	14,389
FY 98	3C	49	54	87	14,181	13,285
FY 99*	3C	33	65	85	14,301	12,890

Remarks: This table provides an overall view of the 3C career field. The tables following provide breakdowns by each individual Air Force specialty.

Table 14. Computer-Computer Systems Operations (3C0X1)

Year	Skill	1 st Term %	2 nd Term %	Career %	Billets	Inventory	SRB
FY 96	3COX1	60	71	95	N/A	8,100	.5/.5/0
FY 97	3COX1	55	63	92	8,163	7,710	1/1.5/0
FY 98	3COX1	58	56	90	8,223	7,311	2/3.5/1
FY 99*	3COX1	37	72	86	8,262	7,226	2/4/1

*FY99Q1; N/A – not available

Remarks: This skill area consists of Communication-Computer operators who are performing network administration and/or information assurance functions in network control centers, as well as PC and network repairs. This skill area is undermanned, and retention has not met expectations among all terms over the last three years. SRB has been offered and increased each year.

Table 15. Computer-Computer Systems Programming (3C0X2)

Year	Skill	1 st Term %	2 nd Term %	Career %	Billets	Inventory	SRB
FY 96	3COX2	66	61	83	2,847	2,702	.5/.5/0
FY 97	3COX2	45	44	87	2,435	2,588	.5/.5/0
FY 98	3COX2	32	28	79	1,911	2,005	2/3.5/1.5
FY 99*	3COX2	15	46	67	1,890	1,937	2/4/.5

*FY99Q1

Remarks: This skill area consists of software programmers. Retention has not met expectations among all terms over the last three years. SRB has been offered.

Table 16. Radio Communications Systems (3C1X1)

Year	Skill	1 st Term %	2 nd Term %	Career %	Billets	Inventory	SRB
FY 96	3C1X1	76	81	95	N/A	1,166	0/0/0
FY 97	3C1X1	53	83	94	974	987	0/0/0
FY 98	3C1X1	55	82	96	879	858	0/0/0
FY 99*	3C1X1	25	71	93	875	858	0/0/0

*FY99Q1; N/A – not available

Remarks: This skill area consists of radio operators who manage radio networks. No SRB is offered; however, the current retention trend is being monitored closely.

Table 17. Electronics Spectrum Management (3C1X2)

Year	Skill	1 st Term %	2 nd Term %	Career %	Billets	Inventory	SRB
FY 96	3C1X2	-	66	90	N/A	81	0/0/0
FY 97	3C1X2	-	75	91	76	83	0/0/0
FY 98	3C1X2	-	33	100	77	87	0/0/0
FY 99*	3C1X2	-	100	100	77	89	0/0/0

*FY99Q1; N/A – not available

Remarks: This skill area consists of Electromagnetic Spectrum Managers. They coordinate the use of frequencies within the electronic spectrum. There are no first-term billets in this skill area.

Table 18. Computer-Computer Systems Control (3C2X1)

Year	Skill	1 st Term %	2 nd Term %	Career %	Billets	Inventory	SRB
FY 96	3C2X1	54	56	88	N/A	2,220	1.5/1/0
FY 97	3C2X1	48	51	86	2,169	1,988	1.5/2/0
FY 98	3C2X1	47	23	85	2,156	1,891	2/.3/.5
FY 99*	3C2X1	31	46	90	2,166	1,843	2/4/1

*FY99Q1; N/A – not available

Remarks: This skill area consists of Communications Tech Controllers who also work in network control centers. This skill area is more technically oriented than the 3C0X1 career field and work communications circuits. This skill area has been undermanned over the last three years, and retention has not met Service expectations. SRB has been offered.

Table 19. Planning and Implementation (3C3X1)

Year	Skill	1 st Term %	2 nd Term %	Career %	Billets	Inventory	SRB
FY 96	3C3X1	86	70	98	746	767	1/1/0
FY 97	3C3X1	59	83	95	728	722	1/1/0
FY 98	3C3X1	53	54	87	693	656	1/1/0
FY 99*	3C3X1	60	83	94	695	653	1/2/0

*FY99Q1

Remarks: This skill area consists of communications-computer plans and implementation specialists. They manage communications-computer projects, working with base organizations to ensure work is scheduled and projects are completed. With increased numbers of projects involving networks or adding systems to networks, these personnel have become integral to planning and implementing networks at bases. Retention has gradually declined over the last three years. SRB has been offered.

Officers

The primary IT career field in the Air Force is Communications & Information Systems Officer (33S). Officers in the career field 33S specialize as either Communications & Information (33SX) Officers or Communications/Computer Engineers (33SXA). Each has an established career path and progression. Issues within the officer workforce have included career field progression, adequate training, and retention. To assist in dealing with various community issues, the Air Force stood up an O-6 Steering Group that made several recommendations that were adopted, including development of an officer career guide, assigning more officers to operational missions as their first assignment, and improving basic and advanced officer training. Additionally, the 33SXA officer career path was changed to merge with the 33S community at the O-4 level.

Retention is an issue within the Air Force Officer IT career workforce, particularly with 33SXA officers. The Air Force is pursuing bonuses for all 33S captains, and is allowing captains non-selected for promotion to stay in the Service to 20 years, and majors non-selected for promotion to stay in the Service to 24 years.

The 33S community is receiving its fair share of officers as compared to other mission support career fields in the Air Force. However, retention has been consistently lower than other mission support career fields over the past three years.

The following tables provide retention rates and manning data for officer career fields.

Table 20. Communications and Information Officer (33S)

Year	Skill	CPT %	Mission Support %	Billets	Inventory	Overall Manning
FY 96	33S	39	62	5,025	4,425	88
FY 97	33S	43	68	5,054	4,821	95
FY 98	33S	34	64	4,720	4,419	93
FY 99*	33S	58	58	4,613	4,087	88

*FY99Q1

Remarks: The Air Force measures retention at the O-3 level as its benchmark to meet end-strength/career field requirements. Mission support information is provided as a comparison tool.

Table 21. Communications and Information Systems (33SX)

Year	Skill	Billets	Inventory
FY 96	33SX	4,603	4,094
FY 97	33SX	4,657	4,535
FY 98	33SX	4,371	4,170
FY 99*	33SX	4,282	3,866

*Q1 FY 99

Remarks: The Air Force does not track retention for 33SX officers separately.

Table 22. Communications/Computer Systems Engineer (33XSA)

Year	Skill	Billets	Inventory
FY 96	33SXA	422	331
FY 97	33SXA	397	286
FY 98	33SXA	349	249
FY 99*	33SXA	331	221

*Q1 FY 99

Remarks: The Air Force does not track retention for 33SXA officers separately. Manning has been a concern.

Army

Enlisted

Career Management Field (CMF) 74 is the Army's enlisted career field for Information Operations. Military Occupational Specialties (MOSs) within CMF 74 include Information Systems Operator Analyst (74B), Telecommunications Operator-Maintainer (74C), Telecommunications Computer Operator-Maintainer (74G), and Information Systems Chief (74Z). Personnel enter the career field in MOS 74B, 74C, or 74G, and can expect to progress in rank from E1 to E7. Each MOS merges into MOS 74Z beginning at E8 and progressing through E8 to E9.

Assignments and promotions are made at the Personnel Command (PERSCOM) in Alexandria, Virginia. Force structure is the responsibility of the Office of the Chief Signal at Fort Gordon, Georgia.

The Army has not experienced significant shortfalls in meeting end-strength requirements. The Army offers SRB as a reenlistment bonus, and has allowed personnel to laterally convert from other MOSs to MOS 74. This year, the Army established a target of 125 billets for lateral conversion to MOS 74, and filled 118 within the first two weeks. Like the other Services, the Army does allow prior-service personnel to return to MOS 74, and uses educational programs such as tuition assistance as a reenlistment tool.

Accessions for MOS 74 have not been an issue. Personnel are easily recruited by the recruiting command and accession goals met despite the fact that this particular specialty is not offered an enlistment bonus or the Army College Fund.

The following tables provide retention rates by terms of enlistment by MOS.

Table 23. Information Systems Operator Analyst (74B)

Year	Skill	1 st Term %	2 nd Term %	Career %	Billets	Inventory	SRB
FY 96	74B	51.5	71.8	66.4	2,386*	2,248*	0/0/0
FY 97	74B	59.7	67.2	64.7	2,373	2,350	0/0/0
FY 98	74B	55.2	64.8	45.8	2,481	2,395	1/1/0
FY 99*	74B	47.1	70.6	70.0	2,780	2,484	1/1/0

*Projected Data

Remarks: Overall, retention among 74B personnel has been close to the Army average for first-term personnel. Retention among second-term and career personnel has not been an issue either. There have been some periodic shortfalls within the community when billet increases have been authorized.

Table 24. Telecommunications Operator-Maintainer (74C)

Year	Skill	1 st Term %	2 nd Term %	Career %	Billets	Inventory	SRB
FY 96	74C	35.1	62.9	59.3	2,615*	2,630*	0/0/0
FY 97	74C	57.1	75.7	56.1	2,527	2,398	1/0/0
FY 98	74C	65.7	65.6	42.4	2,425	2,240	.5/0/0
FY 99*	74C	52.7	67.9	60.2	1,955	1,938	1/0/0

*Projected Data

Remarks: Overall, retention among 74C personnel has been close to the Army average for first-term personnel. Retention among second-term and career personnel has not been an issue either. Some billet decreases have been observed and are expected to continue as the Army switches from Autodin to DMS.

Table 25. Telecommunications Computer Operator- Maintainer (74G)

Year	Skill	1 st Term %	2 nd Term %	Career %	Billets	Inventory	SRB
FY 96	74G	41.4	65.4	60.6	372*	382*	0/0/0
FY 97	74G	37.5	57.1	43.3	376	317	1/0/0
FY 98	74G	43.8	66.7	41.2	362	338	0/0/0
FY 99*	74G	42.9	55.6	80	320	325	0/0/0

*Projected Data

Remarks: Overall, retention among 74G personnel has been close to the Army average. This skill area will be gradually phased out over the next two years, and most personnel will be absorbed into FA 74G. Some additional training may be required.

Table 26. Information Systems Chief (74Z)

Year	Skill	Career %	Billets	Inventory	SRB
FY 96	74Z	37.3	120*	114*	0
FY 97	74Z	43.5	119	120	0
FY 98	74Z	37.9	133	153	0
FY99*	74Z	47.8	137	127	0

*Projected Data

Remarks: Retention has not been an issue within MOS 74Z.

Officers

Under OPMS XXI, which was implemented in 1998, development of company grade officers will continue to follow the same pattern as it does today. Upon selection to Major, however, OPMS XXI restructures the Army competitive category by grouping interrelated branches and functional areas into management categories (Career Fields). Officers will be developed, managed, and promoted with other officers in the same Career Field. Each Career Field has its own distinct development track for officers, with varied branch qualification requirements for professional military education, civil schooling, training, and military experience. The Army established the Information Operations (IO) Career Field (CF) within a four Career Field based management system, to respond to requirements of the 21st century information age. The IO CF brings together information-related disciplines (Functional Areas) by combining existing functional areas and new ones into a single CF. Included in these disciplines is FA 53 (Information Systems Management) that currently exists as an IT occupational specialty and a new IT specialty FA 24 (Information Systems Engineer) that is being established. Branch 25A (Signal Information Systems), though separate, is an IT-related career field. Within the Warrant Officer occupational specialties, there are MOSC 250B (Tactical Automated Network Technician) and MOSC 251A (Data Processing Technician).

There are no special retention and/or incentive pays for any of the officers in the IT-related career fields. However, private sector opportunities and OPTEMPO is straining retention goals among company grade BR 25's officers.

The following tables provide selective retention data for officer career fields.

Table 27. Information Systems Management (AOC 53A)

Year	Skill	MAJ %	LTC %	COL %	Billets	Inventory
FY 96	53A	84.6	75.0	100	476	1,499 (74)
FY 97	53A	82.0	96.3	50	467	1,454 (79)
FY 98	53A	92.8	83.3	50	462	1,375 (85)
FY 99	53A	N/A	N/A	N/A	431	1,256 (136)

() – single-tracked personnel

Remarks: FA 53s billet structure begins at Major. Prior to implementation of OPMS XXI, FA 53 consisted of officers who were “single-tracked” (i.e., serve in only FA 53 billets) and officers who were “dual-tracked” (serve in alternating tours between a primary field (e.g., infantry) and secondary field (e.g., automation)). Use of both types of officers ensured that there was adequate manning to meet the Army’s requirements, and a 2 to 2.5 to 1 ratio in total number of officers was desired. With the initiation of OPMS XXI, the “dual-track” system will be phased out. Officers will serve from their tenth year of service until retirement in their technical field. These officers will compete for promotion against other technical officers only. Overall, this will result in better developed and trained IT officers and higher promotion potential.

Table 28. Signal (Information Systems) Operations (AOC 25A)

Year	Skill	LT %	CPT %	MAJ %	LTC %	COL %	Billets	Inventory
FY 96	25A	90.7	87.7	87.0	88.8	86.7	2,740	2,841
FY 97	25A	90.9	87.4	91.4	92.6	84.3	2,745	2,759
FY 98	25A	90.3	88.3	95.0	89.0	82.8	2,761	2,772
FY 99*	25A	96.2	95.7	97.1	91.7	91.7	2,681	3,453

*As of March 1999

Remarks: FA25A officers work at all levels of command and staff and are engaged in the installation, operation, administration, and maintenance of information systems. FA 25A retention has closely paralleled Army retention rates over the last three years. The Service is concerned over manning at the captain level due to decreases in the continuation rates of captains. Several initiatives are being taken to reverse attrition trends.

Table 29. Network Management Technician (MOS 250N)

Year	Skill	WO1 %	CWO2 %	CWO3 %	CWO4 %	CWO5 %	Billets	Inventory
FY 96	250N	N/A	93	83	78	100	340	296
FY 97	250N	100	93	91	82	100	303	276
FY 98	250N	100	88	70	76	100	295	251
FY 99	250N	100	92	89	96	90	295	242

Remarks: MOS 250N warrant officers manage computer networks at major installations. Retention is monitored closely. Contributing factors are the relatively few numbers of personnel and retirement eligibility at the CWO3 paygrade.

Table 30. Automation Technician (MOS 251A)

Year	Skill	WO1 %	CWO2 %	CWO3 %	CWO4 %	CWO5 %	Billets	Inventory
FY 96	251A	N/A	94	89	75	N/A	115	98
FY 97	251A	100	90	70	72	100	110	77
FY 98	251A	100	94	80	88	100	110	82
FY 99	251A	100	100	60	80	0	115	104

Remarks: MOS 251A officers are data processing technicians and are normally assigned to major headquarters/staffs to ensure automation needs are met. Retention is monitored closely. Relatively few numbers of personnel in the career field and retirement eligibility at the CWO3 level are contributing factors. There is only one billet at the CWO5 level.

Navy

Enlisted

Over the past three years, the Navy has conducted an extensive review/restructuring of its enlisted IT career force. This resulted in the merger of the Data Processor (DP) rating and the Radioman (RM) rating into the RM rating, and creation of new NECs (Naval Enlisted Classification) to meet the needs of IT requirements. New NECs include the following:

- Information Systems Administrator (NEC 2735)
- Network Security Vulnerability Technician (NEC 2780)
- Information Systems Security Manager (NEC 2779)
- Advanced Network Analyst (NEC 2781)

The Navy manages its enlisted IT career force through NECs sourced from different enlisted ratings. The primary rating that sources the IT career field is Radioman (RM). However, other career fields such as Firecontrol Technician (FT) and Cryptologic Technician (CT) can earn IT NECs. IT NECs may be earned by completing formal training or a combination of formal training, on-the-job training (OJT), and experience. The Navy normally tracks personnel retention by their source rating. Overall management of the IT NECs is done by an Enlisted Community Manager. However, it should be noted that a sailor may possess more than one NEC and this complicates tracking personnel retention by NEC. However, personnel with an IT NEC can normally (but not always) expect to be assigned to a billet requiring their respective NEC.

Extensive restructuring has resulted in a dramatic increase in the numbers of billets requiring personnel with an IT NEC. For this reason all of the IT NECs appear undermanned. The Navy is currently growing its workforce to match requirements but does not expect to meet them for the next two to three years. The rate at which the schoolhouses can train personnel will determine how quickly requirements can be met.

In addition to structuring its workforce, the Navy has restructured its schoolhouses for the new NEC requirements. Details are provided in the tables below.

The Navy has offered SRB for specific NECs. Given anecdotal feedback, the Navy assesses that the FY 99 SRB offering is having the desired effect. To boost retention, experience, and competency of its workforce, the Navy is pursuing commercial certification for sailors, advanced education programs such as tuition assistance, and accepting lateral conversions from other career fields into IT NECs.

The following tables provide statistical data for specific NECs.

Table 31. Radioman

Year	Skill	1 st Term %	2 nd Term %	Career %	Billets	Inventory	SRB
FY 96	RM	42.7	56.4	57.3	13,210	12,324	2.0/0/0
FY 97	RM	40.7	57.8	55.0	11,353	11,337	3.0/0/0
FY 98	RM	36.5	52.3	51.4	12,176	11,315	3.5/0/0

Remarks: The RM rating merged with the DP rating in October 1998. The DP rating was the primary IT source prior to the merger. Data for the DP rating prior to the merger is not available. RM retention figures for FY 99 are higher than Navy averages of 27.7% (1st Term), 43.2% (2nd Term), and 37.7% (Career).

Table 32. Information Systems Administrator (NEC 2735)

Year	Skill	Billets	Inventory	SRB
FY 98	2735	1798	668	4.5/2.5/1.5
FY 99	2735	TBD ⁽¹⁾	TBD ⁽¹⁾	4.5/3.0/2.0

(1) Pending the results of a manpower review due in FY 99.

Remarks: This NEC (created in FY 98) fulfills requirements for trained technicians to administer information systems. The focus is on network administration, to include a working knowledge of network operating systems. The target groups of sailors are paygrades E-4/5, with at least three years of fleet/field IT experience. The NEC is currently growing inventory to match the billet base. Because of schoolhouse throughput limitations, the NEC may currently be earned through OJT (subject to certain restrictions).

Deploying battle group IT personnel are being taught a six-week systems administrator course that is bringing them up to speed on the IT systems being installed on their ships. Personnel are not awarded an NEC, but with added experience, they may receive it via OJT.

Table 33. Network Security Vulnerability Technician (NEC2780)

Year	Skill	Billets	Inventory	SRB
FY 98	2780	307	16	
FY 99	2780	TBD ⁽¹⁾	16	5.0/3.0/2.0

(1): Pending the results of a manpower review due in FY 99.

Remarks: This NEC fulfills the requirement for trained technicians to secure information systems. The focus is on all facets of INFOSEC and IO Protection, to include information computer security and expansion, system protection, Windows Clients security management, Novell security management, Microsoft Exchange server security, common Unix threats and security tools, protocols and services, router security configuration, firewall configuration, and secure network server configuration. The targeted group is Sailors in paygrades E-5 through E-8 with extensive fleet/field experience as a systems administrator. Inventory is being grown to match the billet base.

Table 34. Information Systems Security Manager (NEC 2779)

Year	Skill	Billets	Inventory	SRB
FY 98	2779	TBD ⁽¹⁾	1	3.5/2.0/1.0
FY 99	2779	TBD ⁽¹⁾	3	0*

*Expected to be offered in FY 00.

(1): Pending the results of a manpower review due in FY 99.

Remarks: This NEC (created in FY 98) is geared toward E-7 to E-9 personnel and fulfills the requirement for trained technical managers to oversee information systems. Focus of the NEC is network policy and oversight with emphasis on performance vice awareness, to include policy, IW/IO/IA, data encryption, vulnerabilities and countermeasures, security tools, auditing and access control management, life cycle and configuration management, risk analysis, contingency planning, and certification and accreditation.

Personnel must be qualified as either an NEC 2735 or 2780 (or civilian equivalent) as a prerequisite. The course is three weeks in length. The first course is in progress, and is taught in Pensacola, Florida. Mobile Training Teams will teach future courses at fleet concentration areas. Officers and civilians may receive this training if job requirements dictate.

Table 35. Advanced Network Analyst (NEC 2781)

Year	Skill	Billets	Inventory	SRB
FY 98	2781	TBD	1	0
FY 99	2781	TBD		

Remarks: This NEC (created in FY 98) fulfills the requirement for trained technicians to manage information systems. The focus of the NEC is network management across

heterogeneous operating systems, to include systems design, hardware and software installation, system maintenance, network performance optimization, and enterprise networking labs. Targeted sailors are those in paygrades E-6 through E-8, with 2735 fleet/field experience. The course is five weeks in length and is currently taught in Dam Neck, Virginia. SRB will be offered starting in FY00.

Officers

Unlike the other Services, the Navy does not have a specific career field for officers in IT. Rather, the Navy manages its officer IT workforce through a subspecialty system. There are several subspecialties (see table below) in IT and billets have been programmed from Ensign to Admiral. Officers in other career fields acquire an IT subspecialty by acquiring advanced education, experience, or both. The Navy's goal is to assign an officer who has an IT subspecialty to billets identified for an IT subspecialist in at least every other tour.

Table 36. Navy Officer IT Subspecialties

0045X	Command and Control (C2)
0046X	Information Warfare (IW)
0076X	Space Systems Operations
0089X	Information Technology Management
0091X	Computer Science

The Navy reviewed its management of the IT workforce over the past couple of years. There is no single career path (designator) that provides officers to the IT workforce. IT officers come from various designators and filling subspecialty billets such as IT rarely drives assignments.

This has led to concern that the right person may not always be available to fill an IT billet. In an effort to ameliorate this problem and produce more broadly educated IT subspecialists, the Navy (N6) has consolidated the IT related curricula at the Naval Postgraduate School (NPS) into a single curriculum with specialty tracks. This will ensure all graduates of any specific tracks have a common core of knowledge that will enable them to perform effectively in any IT subspecialty billet.

N6 has also sponsored a new IT curriculum at NPS that focuses on the warfighter and is designed specifically for the unrestricted line (warfare) designators. The Navy tracks retention by designator. Since there is no IT designator, tracking retention of personnel with IT subspecialties is difficult. The Navy is reviewing the possibility of merging some other career fields into an IT designator, but no decision has been reached at this time.

In addition to curricular changes at NPS, the Navy has installed an IT curriculum at the Naval Academy and developed a Center for Executive Education at NPS where it offers senior-level (Flag and SES) personnel courses in Information Age issues. The Navy has also undertaken a review of the IT billet structure to ensure billets are properly coded, and the

N6 organization is now actively interfacing with the assignment of officers at the Naval Personnel Command to ensure the most qualified officers are assigned to IT related billets.

The Navy also has the Limited Duty Officer (Designator 6420) and Chief Warrant Officer (Designator 7420) communities who serve as Automated Data Processing (ADP) Officers on large ships (e.g., aircraft carriers and large amphibious ships) and major shore installations. There are 32 LDO 6420 billets and the manning has been maintained over 100% over the last three years (currently at 117%). There are 42 CWO 7420 billets and manning has been maintained at 100% as well. Both groups are sourced from the enlisted ranks and a vast majority has greater than 15 years of active duty service. Retention has not been an issue.

Table 37. Navy Officer Subspecialties – Billets vs. Inventory

IT Subspecialties	O1-3 Billets	O1-3 OFF	O4 Billets	O-4 OFF	O5 Billets	O-5 OFF	O6 Billets	O-6 OFF
0045X	43	20	27	68	61	95	38	60
0046X	31	26	81	58	54	102	3	46
0076X	60	79	44	120	32	115	8	52
0089X	488	272	128	353	111	294	41	103
0091X	61	63	44	96	29	70	4	25
Total	683	460	324	695	287	676	94	286

Remarks: A 3 to 1 ratio between officers and billets is desired.

Marine Corps

Enlisted

The Marine Corps initiated a restructure of its Information Technology career fields approximately two years ago. This resulted in the merger of the Communications Officer and Data Systems Officer into the Communication Information Systems Officer. Similar actions to merge the Communications and Data Systems enlisted fields are in progress. MOSs discussed here reflect the current pre-merge status. Small Computer Systems Specialist (MOS 4066) is now the primary MOS for enlisted personnel. A Small Computer Systems Specialist receives eight weeks of formal IT training at Twenty-nine Palms, California, with approximately one week of focused IA training. A Marine in this career field may progress from E-1 to E-9.

Computer Security Specialist (MOS 4075) and Data Network Technician (MOS 4068) are two additional MOSs that may be earned upon completion of follow-on schooling. These MOSs are managed as subspecialties and not separate career fields.

A challenge the Marine Corps faced in restructuring its enlisted career fields is in training. The basic training provided to a Small Computer Systems Specialist is broad based but not

specific enough in any one area. As a result, the Marine Corps is now reviewing the curriculum and is examining options that would allow more specialization at the entry level, including an IA MOS. Additionally, the Marine Corps is also investigating distance learning and commercial training to address the many emerging IT requirements.

Overall, first-term population and retention are a concern for the Marine Corps. SRB has been offered although retention rates among first-term enlisted personnel have been relatively low. Careerist retention is also becoming a concern as well, particularly at the 8 to 12 year mark. A noticeable reduction in careerists staying in the Marine Corps past the 20-year point has been observed, and the Marine Corps is now offering zone "C" SRB through the remainder of FY 00. In FY 99, the Marine Corps is projecting that end-strength requirements will be met, but believes it will have a 5 to 25% shortfall in meeting the IT workforce requirements (depending on paygrade).

The following table provides retention information for the enlisted MOS.

Table 38. Small Computer Systems Specialist (MOS 4066)

Year	Skill	1 st Term %	2 nd Term %	Career %	Billets	Inventory	SRB
FY 96	4066	117	107	133	880	1,010	4/0/0
FY 97	4066	67	95	104	1,549	1,211	4/0/0
FY 98	4066	70	103	82	1,526	1,217	4/0/0
FY 99*	4066	81	88	93	1,545	1,302	4/3/0

*As of Jan 99

Remarks: The Marine Corps tracks retention in several ways; the most prevalent is based on a tool known as "grade adjusted recapitulation" or GAR, which accommodates all billet requirements as well as other "overhead requirements" such as entry level training, recruiting duty, and drill instructor duty. The figures above reflect the total workforce on hand vs. GAR. The Marine Corps strives to maintain GAR at 85% to 110%. During FY 97, the number of billets in the 4066 MOS was increased twice. Therefore, retention numbers appear low for that reason.

Officers

Communication Information Systems Officer (MOS 0602), the primary IT career field for officers, was formed three years ago by combining the communications and data systems MOSs as noted above. Officers receive 23 weeks of formal school in Quantico, Virginia, with approximately one week focused on IA. Like the enlisted ratings, the training is considered broad based, with not specific enough training in any one area. Consequently, the Marine Corps is reviewing its training curriculum for officers as well. The billet structure for Communication Information Systems Officers allows for a Marine to progress to O-6/O-7 over the course of a career.

Because of the recent formation of the Communication Information Systems Officer MOS, retention has been difficult to ascertain. However, early feedback from Marines in the field points to problems on the horizon.

Table 39. Communications Information Systems Officer (MOS 0602)

Year	Skill	LT %	CAPT %	MAJ %	LTCOL %	Billets	Inventory
FY 96	0602	83	75	64	57	1,043	744
FY 97	0602	63	99	71	66	951	722
FY 98	0602	75	103	77	68	958	789
FY 99	0602	63	95	72	65	958	715

Conclusions

Each of the Services has structured specialties in IT to meet the needs of the respective Service. Overall, the Services are meeting end-strength requirements, but each is increasingly challenged in retaining experienced personnel in both enlisted and officer ranks. There are IT occupational specialties, particularly within the Air Force and Marine Corps, where retention has not met expectations and is a concern.

SRB is used but could be used to a greater extent by the Services in those cases where retention is a concern. Current law and policy allow for maximum SRB payments of \$45,000 and \$30,000 respectively, and a multiple of 10 and 6. In those cases where retention is an issue in the enlisted ranks, SRB is not being maximized, nor have waivers to policy been requested. Internal Service priorities for allocation of SRB funds may be a factor.

There are no continuation incentives for officers similar to those provided to enlisted personnel. For the reasons stated previously and the evolving nature of the IT workforce, long-term continuity appears to be an issue, particularly in the Air Force and Marine Corps. Additional study in this area appears to be warranted and should be conducted to meet FY 02 budget submission requirements should such a study recommend continuation pays be pursued.

Given projected shortfalls of skilled IT personnel in the private sector and a continued robust economy, retention of experienced personnel is expected to be challenging for the foreseeable future. An OSD-sponsored steering group comprising OSD, Joint Staff, and each of the Services should be established to focus on military IT personnel issues. While each of the Services has recognized the challenges in retaining experienced military IT personnel, and is taking actions to address the problems, many of the approaches are not being shared among the Services. Given the long-term situation in the private sector, the Services' retention of experienced personnel is not likely to disappear soon. A steering group would serve to:

- Foster a mutual exchange of information on accession/retention programs related to military IT professionals.
- Focus budgeting strategies (e.g., SRBs, continuation pays, etc.).
- Provide a venue for developing new approaches (e.g., commercial certification incentives in exchange for additional service commitment).
- Develop long-term military IT personnel strategies.

Appendix G. Requirements for IT/IA Coding of DoD Manpower/Personnel Databases

General

The CINCs, Services, and Agencies must code all billets/positions (manpower) and people (personnel) that are assigned IT or IA functions. This coding will be a two-character code.

- The first character will be an Arabic numeral and will represent the IT workforce category. IT Workforce Categories are defined in Attachment 1.
- The second character will be an alpha character and will represent the IA function code.

IA Function Codes are defined in Attachment 2. Although not likely, it is possible that there could be seven occurrences of this data element for any billet/position or person. Except for NSA, DIA, and NIMA, this data element must be included in the data provided to the Defense Manpower Data Center (DMDC) on a recurring basis.

These IT workforce categories and IA function codes apply to all military (active and Reserve Component) and civilian personnel and billets/positions if they meet the conditions specified in the subsequent rules. These function codes are independent of occupational specialties. For example, if a cook is assigned the responsibility of system administration, that person will be given the appropriate IA functional code even though the person is not an IT professional.

The coding of the manpower and personnel data is semi-independent of each other. If a person is assigned an IT and/or an IA function, but this is *not* a responsibility of the billet or position, the personnel file will be coded but the manpower file will not be coded. The reverse is *not* true. If a billet or position is assigned an IT and/or an IA function, the person should be assumed to also be assigned the function. In this case, if the manpower file is coded, then the personnel file must also be coded.

IT codes can be used without IA codes. IA codes always require an IT code.

Codes for both people and positions/billetts will reflect only *current* assignments and will not include past experience and/or qualifications.

Vacant civilian positions assigned an IT and/or an IA function will be coded only if it is a valid position. In other words, it must be an authorized position.

IA Functions

If a person or position/billet is assigned any of the five critical functions (D, G, I, J, or K), *no matter how negligible the % of time*, the person and/or position/billet must be coded for the applicable function(s).

If the person and/or position/billet is assigned Function I, Function D code will be used. In other words, the Function I code will *not* be used (security reasons).

For all other IA functions, the person and/or position/billet will be coded only if the time associated with that function represents 25% or more of the time.

IA codes D, G, H, I, J, K will be assigned an IT code of 4.

IT Functions

A billet/position and/or person cannot be coded in IT codes 1, 2, or 3 simultaneously. Only one or none of these codes can be used on a single billet/position and/or person.

A billet/position and/or person that is coded with IT code 6 cannot be coded with any other IT code.

Attachment 1

Major IT Workforce Categories

1. **CIOs and personnel performing equivalent duties in agencies.** Accountable for all agency information resources management activities, promotes effective agency operations by encouraging performance-based management, and fosters the effective acquisition and use of information technology (IT) in accordance with the Clinger-Cohen Act and other IT-related Acts and Laws. (Detailed critical functions are outlined in the Clinger-Cohen Core Competency list in Appendix C.)
2. **Deputy CIOs and personnel performing equivalent duties in agencies.** Support the CIO in carrying out information resources management activities and acts on the behalf of the CIO in his or her absence.
3. **CIO staff and personnel performing equivalent duties in agencies.** Personnel supporting the activities of the CIO in carrying out the responsibilities of the CIO office.
4. **Technical Personnel such as: (occupational specialties listed below or people or billets/positions performing functions listed under 9.0 of the Clinger-Cohen Core Competencies).**
 - Computer Specialists (including systems/network administrators)
 - Computer Programmers
 - Telecommunications Specialists
 - Computer Engineers
 - General Engineers (General Engineers performing IT functions)
 - Electronic Engineers (Electronic Engineers performing IT functions)
 - Industrial Engineers (Industrial Engineers performing IT functions)
 - Computer Scientists
5. **Information Technology Program/Project Managers /Deputy Program/Project Managers.** Principal official and centralized authority responsible for the management of a specific information technology program throughout the system life cycle. This includes the planning, organizing, staffing, controlling, and leading the combined efforts of participating /assigned civilian and military personnel and organizations.
6. **Personnel performing Information Technology (IT) Functions (These are personnel with primary functions other than IT, but perform some type of IT-related duties at least 25% of their time).** Personnel who spend 25% or more of their time performing IT functions identified on the Clinger-Cohen Core Competencies List

Information Assurance (IA) Functions

All information assurance functions described below include both tactical/deployable systems and strategic or fixed systems. Those that are tied to privileged access are identified as a **CRITICAL FUNCTION** and are shaded.

Function A – IA Certification and Accreditation

- Systems
- People
- Equipment
- Procedures/Policies
- Security

Function B – IA Training/Education

- Professors/Instructors
- Course Developers
- IA Training Administration

Function C – IA Management

- Unit/Base/HQ Levels
- Acquisition of Secure Systems
- Policy/Procedure
- Development
- Implementation
- Compliance
- Enforcement
- Asset Accountability

Function D – System/Network Administration and Operations [critical function]

- Configuration Control
- Installation
- Operations and Maintenance
- System Selection
- Access Control
- Response/Recovery/Reconstitution

- Incident Response
- Operations Monitoring and Analysis
- Countermeasures

Function E – Systems Security Engineering

- Research
- Design
- Development
- IA Planning and Control
- IA Requirements Definition
- IA Design Support
- IA Operations Analysis
- Life Cycle IA Support
- IA Risk Management

Function F – IA Systems/Product Acquisition

- Procurement
- Technical Expertise

Function G – Computer/Network Crime [critical function]

- Forensic Analysis
- Criminal Prosecution/Investigation

Function H – Cryptography

- Operations
- Management

Function I – Threat and Vulnerability Assessment [critical function]

- Red-Teaming
- Penetration Testing
- Threat Analysis

FUNCTION J – COMPUTER EMERGENCY RESPONSE TEAM (CERT) [critical function]

- Clearinghouse for collection of technical vulnerability information
- Clearinghouse for collection of incident reports
- Provide technical expertise to mitigate and reconstitute to victim site following an event/incident

- Disseminate vulnerability information with mitigation solutions (when possible)
- Disseminate threat information
- Coordinate with other CERTs
- Coordinate with appropriate law enforcement agencies
- Coordinate with appropriate counterintelligence agencies

Function K – Web Security [critical function]

- Information management
- Information systems administration
- Information system security

Appendix H.
Certification Requirements for
System/Network Administrators

Table 40. Certification Requirements of System/Network Administration & Operations

Function	Certification		Performance items ⁶ [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Functional Specification			Demo		Sign-off	Certification Validity		Re-Certification
<i>Privileged Access</i>	<i>Pre-Req. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>	<i>NIST</i>		<i>NSTISSI No. 4013</i>	<i>Test</i>	<i>On- the- Job</i>	<i>Cmd.-Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
SA-L1	0-2 Years OS Experience		Know rudimentary system / network administrator tasks relevant to the OS or network device	Manage system hardware & software. Maintain data store	Day-to-day operations	1D, 3.5D	2.2D 3.6D	1, 5	X	X	Supervisor	Every 24 Months	Major Systems Changes (e.g., major updates)	Requirement: OS Certification Required or En route
	Formal training on the OS & CMD language (sys admins) or network protocols & operating parameters (network admins)		Know OS, command language, &/or network protocols	Provide communication connectivity & configure network protocols	Install OSs, applications & peripherals, testing & safeguards	3.2D 3.3D 3.5C	3.5D 3.4D	1(b)					Individual/Station Re-assignments (e.g., OS change)	Policy: Billets must be coded
	Background Investigation (BI)			Maintain expertise									Policy changes	Policy: part time sys admins must be certified
			Know normal operating parameters of relevant systems & applications	Install & verify software patches	Recognize abnormal operations. Recognize potential threats	1D 3.5D	2.2D	1(b)						Policy: maintain certification & re-certification records

⁶ **Note:** This is a list of operational requirements for system & network administrators. Choose applicable Knowledge-Skills-Abilities.

Table 40. Certification Requirements of System/Network Administration & Operations

Function	Certification		Performance items ⁶ [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Functional Specification		Demo		Sign-off	Certification Validity		Re-Certification
			Knowledge	Skills	Abilities	NIST	NSTISSI No. 4013	Test	On-the-Job	Cmd.-Level	Admin.	Other Triggers	Reqs. & Policies
Privileged Access	Pre-Reqs. or Equivalent	Topical Areas or Courses											Policy: Cmdr specifies additional KSA via annual training
				Manage accounts									
			Know basic system & configuration troubleshooting	Troubleshoot problems	Troubleshoot user problems	3.5A 3.5D	3.5C						
					Conduct informal, on-the-spot user assistance & training	2.2D	3.5A	1 (b)					
			Basic knowledge of command's/organization's network										

Table 40. Certification Requirements of System/Network Administration & Operations

Function	Certification		Performance items ⁶ [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Functional Specification		Demo		Sign-off	Certification Validity		Re-Certification
<i>Privileged Access</i>	<i>Pre-Req. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>	<i>NIST</i>	<i>NSTISSI No. 4013</i>	<i>Test</i>	<i>On- the-Job</i>	<i>Cmd.-Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
	Formal training on IA awareness & common system / network vulnerabilities		Know most common vulnerabilities	Ensure security. Protect, detect, react against system incursions	Assist ISSO in access control security (i.e., passwords, auditing & alarming, etc.)	3.3D	1(b) 1(e)						
			Know local IAVA procedures		Understand & react to vulnerability alerts (IAVAs)	1D 3.4C	1(a)						
			Know local procedures for incident reporting & how to contact security assistance		Receive & initiate incident reports	1D 3.5D 2.2D 3.6D	1(a)						
			Know principles of prioritizing customers & systems; understand impact of emergency operations	Interact with others	Assist Skill level 2 sys admins with emergency restoration, surge planning & surge operations.	3.4D 3.5D	1C						
					Install emergency workarounds, as directed	3.5A 3.6D	6(a) 5(a)						

Table 40. Certification Requirements of System/Network Administration & Operations

Function	Certification		Performance items ⁶ [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Functional Specification		Demo		Sign-off	Certification Validity		Re-Certification
<i>Privileged Access</i>	<i>Pre-Reqs. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>	<i>NIST</i>	<i>NSTISSI No. 4013</i>	<i>Test</i>	<i>On-the-Job</i>	<i>Cmd.-Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
			Know basic differences between garrison & deployed (tactical) operating environments										
			Know how to safeguard classified data				1(b) (a) (d)						
			Know about destruction plans & the various events which trigger their execution	Destruction techniques	Assist with emergency destruction planning & execution	3.6D	1 (b) 6 (c)						
SA-L2	2-5 Years OS Experience		Know how to administer the relevant OS & application(s) &/or networks (system administrators). Know telecommunications & key mgmt. (network administrators)	Interact with others	Interact with developers, operations centers, & support personnel to maintain reliable operations. Continually monitor health of system	3.4D 3.5A	5	X	X	Unit CDR	Every 24 Months	Major Systems Changes (e.g., major updates)	Formal training required or Enroute
	Background Investigation (BI)			Manage system hardware & software								Individual/Station Re-assignments (e.g., OS change)	

Table 40. Certification Requirements of System/Network Administration & Operations

Function	Certification		Performance items ⁶ [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Functional Specification		Demo		Sign-off	Certification Validity		Re-Certification
<i>Privileged Access</i>	<i>Pre-Req. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>	<i>NIST</i>	<i>NSTISSI No. 4013</i>	<i>Test</i>	<i>On- the- Job</i>	<i>Cmd.-Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
	Formal training in networking, programming language concepts & algorithms			Solve complex problems	Independently solve complex network/security problems	3.2D 3.4C	4					Policy changes	Policy: part time sys admins must be certified
				Maintain data store. Ensure the validity & reliability of data files	Explain solutions for complex problems to users & other system administrators	3.5A	1 c						Policy: maintain certification & re-certification records
	Program in a command language (sys admins)				Train Skill Level 1 sys admins	3.5A	1c						Policy: Cmdr specifies additional KSA via annual training
	Formal training in firewall mgmt., intrusion detection, & security tools		Know associated vulnerabilities of command/s/organization's interconnected & interdependent systems	Maintain expertise. Maintain current knowledge on network vulnerabilities & solutions	Systematic & continuous inspection IAW technical & security standards	2.2D 3.4D 3.5C	4c, 3a						
	Strong communications & customer relations skills		Know networking, algorithms, & program language concepts. Know how to program in a command language; know telecommunications networking, key mgmt., network design, configuration, & interconnections		Implement complex OS changes	3.2D 3.4C	5a, c						

Table 40. Certification Requirements of System/Network Administration & Operations

Function	Certification		Performance items ⁶ [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Functional Specification		Demo		Sign-off	Certification Validity		Re-Certification
	<i>Pre-Reqs. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>	<i>NIST</i>	<i>NSTISSI No. 4013</i>	<i>Test</i>	<i>On-the-Job</i>	<i>Cmd.-Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
<i>Privileged Access</i>			Know how to implement firewall mgmt., intrusion detection, & available security tools	Ensure security. Protect, detect, react against system incursions.	Monitor & ensure that security hard & software operates properly	3.3D	6, 2 b						
				Manage accounts	With ISSO, plan most effective use of security tools	3.4C	4, 6b						
			Know all interactions within domain. Know how to identify abnormal operations		Analyze threats. Identify differences between technical problems & security incursions	1D 2.2D	5, 3						
					Establish & monitor internal domains & security enclaves	3.4C	1 e						
					Monitor & balance load among servers & networks within the domain. Detect & interpret system abnormalities	3.4D	5c, 6c						

Table 40. Certification Requirements of System/Network Administration & Operations

Function	Certification		Performance items ⁶ [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Functional Specification		Demo		Sign-off	Certification Validity		Re-Certification
<i>Privileged Access</i>	<i>Pre-Req. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>	<i>NIST</i>	<i>NSTISSI No. 4013</i>	<i>Test</i>	<i>On- the- Job</i>	<i>Cmd.-Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
				Troubleshoot Problems	Complex troubleshooting across all networks	3.4D							
					Scope, plan & implement countermeasures	3.5C 3.5D	2b,c 3b						
			Comprehensive knowledge of command's/organization's network & primary external & internal connectivity	Provide communication connectivity	Plan, supervise, implement, & inspect rapid assimilation of surge (crisis) networks	3.4D 3.5A	5a, 6						
			Know command/agency's mission & priorities. Know command/agency's critical, essential, & support systems		Protect/recover information from loss or damage. Conduct emergency restoral planning & operations	3.5D	5a, 6						
			Know physical & software interfaces for priority systems. Understand alternative/backup systems available for continuity of operations		Plan, supervise, implement, & inspect emergency workarounds & large scale system restorals	3.5D	5a, 6						

Table 40. Certification Requirements of System/Network Administration & Operations

Function	Certification		Performance items ⁶ [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Functional Specification		Demo		Sign-off	Certification Validity		Re-Certification
<i>Privileged Access</i>	<i>Pre-Reqs. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>	<i>NIST</i>	<i>NSTISSI No. 4013</i>	<i>Test</i>	<i>On-the-Job</i>	<i>Cmd.-Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
			Know infrastructure's critical nodes & understand effects of infrastructure failure		Predict crisis/attack vulnerabilities & losses, to include impact of failed infrastructure & physical destruction of networks/equipment	3.4D 3.5A	5a, 6						
			Know how to prepare for operations in varied environments (garrison, deployed, etc.)	Requisition & maintain equipment stocks for varied operating environments (garrison, field/deployed), as required	Operate in varied environments: garrison, deploying, etc.	3.5C	5a, 6						
					Operate during electronic/physical attack	3.5C 3.4C 3.3D	5, 6						
			Know local procedures for incident reporting & IAVAs		Scope, plan & implement countermeasures from technical vulnerabilities	3.5C 3.5D	1a						
			Know local & DOD security policy & standards. Know how to handle & safeguard classified data		Enforce security policy & procedures. Correct deficiencies	3.4C	5a, 1a						

Table 40. Certification Requirements of System/Network Administration & Operations

Function	Certification		Performance items ⁶ [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Functional Specification		Demo		Sign-off	Certification Validity		Re-Certification
<i>Privileged Access</i>	<i>Pre-Reqs. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>	<i>NIST</i>	<i>NSTISSI No. 4013</i>	<i>Test</i>	<i>On-the-Job</i>	<i>Cmd.-Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
			Know appropriate web security measures				1d						
			Know OPSEC & privacy issues to include policies on WEB release/review		Able to differentiate between appropriate/inappropriate materiel for WEB release	1D 2.2D	1d, 1a						
			Know DoD & local rules of engagement. Working knowledge of legal implications of attack response	Preserve evidence of attack, tampering	Respond to attack IAW rules of engagement & applicable law	1D 3.5A 3.5D	1a						
			Knows about destruction plans & techniques & when to execute	Physical destruction techniques	Plan & implement emergency destruction	3.6D 3.5D 3.5C	6c						
SA-L3	Over 5 Years OS Experience		Knowledge of OS design, data/algorithm structure, machine architecture, networking, programming language, & concepts/algorithms. Know telecommunications, key mgmt., network design, configuration, & interconnection	Expert mgmt. of system hardware/swtware & data store. Expert mgmt. of application software	Take general direction from mgmt. & produce integrated security solutions/designs	3.4C 3.5D	1a b 2a,	X	X	Unit CDR	Every 24 Months	Major Systems Changes (e.g., major updates)	Formal training/ Certification Required or Enroute

Table 40. Certification Requirements of System/Network Administration & Operations

Function	Certification		Performance items ⁶ [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Functional Specification		Demo		Sign-off	Certification Validity		Re-Certification
<i>Privileged Access</i>	<i>Pre-Req. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>	<i>NIST</i>	<i>NSTISSI No. 4013</i>	<i>Test</i>	<i>On-the-Job</i>	<i>Cmd.-Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
	At least 5 years experience administering the relevant OS(s)			Work independently or lead teams to quickly & completely solve problems	Solve complex problems involving external & internal assets/issues. Articulate network & command/agency reqs	3.4C	1a, b					Individual/Station Re-assignments (e.g., OS change)	Policy: Billets must be coded
	Fluent in one or more command language; competent in one		Know applicable programming languages & security vulnerabilities of those languages	Maintain expertise								Policy changes	
	Formal training in OS design, data/algorithm structure, machine architecture, networking, programming, & concepts/algorithms			Ensure security. Protect, detect, react against system incursions									
	Background Investigation (BI)		Understand the strategic view of the network operation/mission, & interaction with all external domains	Provide communication connectivity	Plan & design the security architecture	3.5C 3.4C 3.5D	2, 4						
					Tune the performance of existing domains; monitor for attacks	3.3D	1b						

Table 40. Certification Requirements of System/Network Administration & Operations

Function	Certification		Performance items ⁶ [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Functional Specification		Demo		Sign-off	Certification Validity		Re-Certification
	Pre-Reqs. or Equivalent	Topical Areas or Courses	Knowledge	Skills	Abilities	NIST	NSTISSI No. 4013	Test	On- the-Job	Cmd.-Level	Admin.	Other Triggers	Reqs. & Policies
Privileged Access	Strong interpersonal, organizational, & communications skills		In-depth knowledge of DoD security /IA training reqs..	Interact with others	Train skill levels 1, 2	3.5A	1c						
	Can make proposals & presentations, write plans & orders				Can make presentations, write proposals & plans, & interact with mgmt. & other organizations								
			In-depth knowledge of local, DoD security & IA policies		Set &/or interpret standards, security procedures & safeguards. Identify & rectify policy gaps. Set, adjust audit priorities	3.5A 3.5D	3.5C 3.6D	4c, 3a					
					Advise CDR on IA & INFOSEC issues. Suggest performance & security improvements	3.2D 2.2D	3.3D	3a 2a, b					
					Advise Public affairs & local webmasters on WEB security issues	3.2D 2.2D	3.3D	1d					

Table 40. Certification Requirements of System/Network Administration & Operations

Function	Certification		Performance items ⁶ [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Functional Specification		Demo		Sign-off	Certification Validity		Re-Certification
<i>Privileged Access</i>	<i>Pre-Reqs. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>	<i>NIST</i>	<i>NSTISSI No. 4013</i>	<i>Test</i>	<i>On-the-Job</i>	<i>Cmd.-Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
			In-depth knowledge on limits of response & DOD/local rules of engagement		Analyze IT security laws, vulnerabilities, & recognize the legal ramifications of attack responses. Interpret appropriate rules of engagement	1D 3.4D 3.4C 3.5A	4a, b, c 2c, b						
			Know how to design & implement network defense In-depth. Assess, manage, & plan the countermeasure implementation of a technical vulnerability		Lead teams to tackle complex security problems (certifiers & developers). Plan large scale implementation/installation of security devices & upgrades	3.2D 3.4C 3.3D							
			Know technical & operational implications of outages & interruptions										
			Know potential attack threat(s) & most likely damage. Understand infrastructure vulnerabilities & their potential to affect the network		Predict crisis/attack losses & network vulnerabilities across scope of conflict	3.4D 3.5A	5, 6, 3						
					Conduct systemic analysis of attack implications. Interpret impact of outages & rapidly issue alternative plans	3.4D 3.5A 3.4D	5, 6						

Table 40. Certification Requirements of System/Network Administration & Operations

Function	Certification		Performance items ⁶ [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Functional Specification		Demo		Sign-off	Certification Validity		Re-Certification
<i>Privileged Access</i>	<i>Pre-Reqs. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>	<i>NIST</i>	<i>NSTISSI No. 4013</i>	<i>Test</i>	<i>On- the-Job</i>	<i>Cmd.-Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
			Understand operational priorities & which systems & infrastructures support them		Manage, predict, & rapidly assimilate surge (crisis) users	3.5A	5, 6						
					Integrate tactical & strategic networks & security issues.	2.2D	6a, c						
					Plan & provide materiel for transition to varied operating environments (garrison to deployed, etc.)	3.4C 3.5C	5, 6						
				Destruction techniques	Produce standard & emergency restorral orders, destruction plans, & continuity or operations plans	3.6D	5,6						
			Know user reqs. & network capabilities		Balance user reqs. against network capacities (& mission rqmts)	3.3D 3.5C	1, 5						

Table 40. Certification Requirements of System/Network Administration & Operations

Function	Certification		Performance items ⁶ [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Functional Specification		Demo		Sign-off	Certification Validity		Re-Certification
			Knowledge	Skills	Abilities	NIST	NSTISSI No. 4013	Test	On- the-Job	Cmd.-Level	Admin.	Other Triggers	Reqs. & Policies
Privileged Access	Pre-Reqs. or Equivalent	Topical Areas or Courses	Budget mgmt.		Able to create & manage a budget	2D							

Appendix I.
Certification Requirements for
Threat and Vulnerability Assessments

Table 41. Certification Requirements for Threat & Vulnerability Assessment

Function	Certification		Performance Items [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Func. Spec.	Demonstration		Sign-Off	Certification Validity		Re-Certification
<i>Privileged Access</i>	<i>Pre-Req. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>	<i>NIST</i>	<i>Test</i>	<i>On-the-Job</i>	<i>Cmd. - Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
Threat Assessment; Vulnerability; Red Team	DAA Certification Mandated		Know state-of-the-art security policies & policy models & their applications			NSTISSC 4011	X	X	Unit CDR	Every 18-24 Months	Major Systems Changes (e.g., major updates)	Req.: OS Certification Required or En Route
	SA-L2 Secret Clinc SA-L3 TS Clearance		Knowledge of state-of-the-art security applications both hardware & software			NSTISSC 4012					Individual/Station Re-assignments (e.g., OS change)	Policy: Billets must be coded
	Background Investigation		In-depth knowledge of principles of cryptography & applicable methods									
			Know data communications technologies such ATM, Ethernet, etc.; ISO/OSI transmission standards; ATM transmission standards		Recognize abnormal operations. Recognize potential threats							
			In-depth training on applicable OS(s)	Highly skilled in configuring & operating OS for security								
			Good understanding of state-of-the-art in Firewalls, Routers, Bridges, network & host-based intrusion detection systems, etc.									
			Thorough knowledge of current "approved security products."	Troubleshoot Problems	Troubleshoot user problems							Policy: Cmdr specifies additional KSA via annual training

Table 41. Certification Requirements for Threat & Vulnerability Assessment

Function	Certification		Performance Items [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Func. Spec.	Demonstration		Sign-Off	Certification Validity		Re- Certifica- tion
<i>Privileged Access</i>	<i>Pre-Req. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>	<i>NIST</i>	<i>Test</i>	<i>On-the- Job</i>	<i>Cmd. - Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
			Knowledge & understanding of National & local/agency policies (including legal aspects)									
			Good knowledge of current & past hacking techniques	Maintenance of currency in re-CERT, IAVAs, & vendor bulletins								
			Know Threat, Vulnerability, Risk Mgmt. tools, methods, & policies		Ability to plan exploitation operation to include impact on network under attack							
			Know Monitoring rules, regulations, laws, & methods									
			As required, know & understand steganography, malicious logic, & other esoteric "stuff"									
				Conduct vulnerability assessment/online survey & interpret results	Coordinate, create & deliver in-brief & out-brief to appropriate personnel							
			Know & understand selected ISSO functions such as account mgmt., audit reviews, underlying policies/models currently in use									
			Understand coordination procedures for computer network vulnerability assessments/online surveys									

Table 41. Certification Requirements for Threat & Vulnerability Assessment

Function	Certification		Performance Items [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Func. Spec.	Demonstration		Sign-Off	Certification Validity		Re-Certification
<i>Privileged Access</i>	<i>Pre-Req. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>	<i>NIST</i>	<i>Test</i>	<i>On-the-Job</i>	<i>Cmd. - Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
			In-depth working knowledge of network & host-based intrusion detection systems & network monitoring devices									
			Types of attacks used by intruders against systems & networks & implications for risk assessment	Highly skilled in analyzing attacks against systems & networks								
			In-depth working knowledge of exploitation tools & techniques used by Intruders	Highly skilled in use of tools & techniques to counter attacks against systems & networks in accordance with incident handling policies/procedures								
			Technical knowledge of HW/SW vulnerabilities of OSs &/or DBMS (Team may be made up of individuals each w/unique knowledge of a different OS)	Analyze computer network configuration from security point of view	Ability to lead smaller teams to solve complex security problems							
			In-depth technical knowledge of the internet & web protocols, applications, services, security issues, & host/system security issues		Ability to identify common vulnerabilities in web products, i.e. HTML code & CGI, PERL, & JAVA							
				Very strong interpersonal, organizational, & communication skills. Can make presentations, write proposals & plans, & interact with mgmt. & other organizations.	Explain complex problems, events & solutions to senior mgrs. & decision makers							

Table 41. Certification Requirements for Threat & Vulnerability Assessment

Function	Certification		Performance Items [Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]			Func. Spec.	Demonstration		Sign-Off	Certification Validity		Re- Certifica- tion
			Knowledge	Skills	Abilities							
<i>Privileged Access</i>	<i>Pre-Req. or Equivalent</i>	<i>Topical Areas or Courses</i>				<i>NIST</i>	<i>Test</i>	<i>On-the- Job</i>	<i>Cmd. - Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Req. & Policies</i>
			In-depth knowledge of DOD critical infrastructure (DCIP) & priority systems & networks									
					Advise higher mgmt. on IA & INFOSEC issues & recommend performance & security improvements.							

Appendix J.
Certification Requirements for
Computer Emergency Response Team

Table 42. Certification Requirements for CERT

Function	Certification		Performance Items			Func. Spec.	Demonstration		Sign-Off	Certification		Re- Certification
			[Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]							Validity		
<i>Privileged Access</i>	<i>Pre-Reqs. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>		<i>Test</i>	<i>On-the-Job</i>	<i>Cmd. - Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
CERT-L1 (Help Desk)	2-5 Years OS Experience	Incident Handling Course	CERT policies & procedures for handling incidents, including documentation & reporting (National, DOD, local)	Highly skilled in quickly identifying nature of customer problem & accurately determining its significance	Ability to communicate effectively through written communication		X	X	CERT Mgr.	Every 18-24 Months	Major Systems Changes (e.g., major updates)	Requirement: OS Certification Required; CERT Certification Required
	SA-L2		Knowledge of core security principles, concepts, applications, services & issues		Ability to communicate effectively through oral communication						Individual/ CERT Reassignment (e.g., OS change)	Policy: Billets must be coded
	Background Investigation		Knowledge of INFOCON stages & requisite responses/actions at each stage		Ability to effectively explain, advise & direct implementation for each INFOCON level							
					Ability to follow policies & procedures							
					Ability to function effectively in a dynamic team environment							Policy: CERT Mgr. specifies additional KSA via annual training
CERT-L2 (Incident Handler)	CERT-L1	Incident Handling Course	Types of attacks used by intruders against systems & networks & implications for risk assessment	Highly skilled in analyzing attacks against systems & networks	Accurately document & report incidents		X	X	CERT Mgr.	Every 18-24 Months	Major Systems Changes (e.g., major updates)	OS Certification Required or Enroute
	Background Investigation	Vendor workshops, conferences, discussions,	In-depth working knowledge of tools & techniques used by Intruders	Highly skilled in use of tools & techniques to counter attacks against systems & networks in accordance with incident handling policies/procedures	Ability to employ appropriate countermeasures to effectively achieve desired outcome						Individual/Station Re- assignments (e.g., OS change)	Billets: must be coded

Function	Certification		Performance Items			Func. Spec.	Demonstration		Sign-Off	Certification Validity		Re-Certification
			[Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]							Admin.	Other Triggers	
Privileged Access	Pre-Reqs. or Equivalent	Topical Areas or Courses	Knowledge	Skills	Abilities		Test	On-the-Job	Cmd.-Level	Admin.	Other Triggers	Reqs. & Policies
			Technical knowledge of HW/SW vulnerabilities of OSs (Team may be made up of individuals each w/unique knowledge of a different OS)		Ability to lead smaller teams to solve complex security problems							Policy: Cmdr specifies additional KSA via annual training
			In-depth technical knowledge of the internet & web protocols, applications, services, security issues, & host/system security issues		Ability to analyze IAVA & other data & make a determination of the health of the Team's overall system/ network(s)							
				Highly skilled in configuring & operating OS for security								
					Test & evaluate incident handling countermeasures, including procedures, policies, tools & techniques							
			Incident Handling organizations & structure at Local, DOD, Federal, National, International levels		Ability to work as a member of a team which includes external sites & elements							
			Working knowledge of legal aspects of incident handling/attack response									
			Knowledge of the role & responsibilities of law enforcement in computer incidents									

Function	Certification		Performance Items			Func. Spec.	Demonstration		Sign-Off	Certification Validity		Re-Certification
			[Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]							Certification Validity		
<i>Privileged Access</i>	<i>Pre-Reqs. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>		<i>Test</i>	<i>On-the-Job</i>	<i>Cmd. - Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
CERT-L3 (Mgr.)	At least 5 Years OS Experience				Interact with vendors, other CERTs, others to enhance security features of HW/SW		X	X	Unit CDR	Every 18-24 Months	Individual/ Station Reassignment	OS Certification Required
	2-3 years CERT Incident Handling experience				Set local incident handling SOPs, & rules of engagement							Billets: must be coded
	SA-L3/ CERT-L2			Very strong interpersonal, organizational, & communication skills. Can make presentations, write proposals & plans, & interact with mgmt. & other organizations.	Explain complex problems, events & solutions to senior mgrs. & decision makers							
	Top Secret Clearance		In-depth knowledge of DOD critical infrastructure (DCIP) & priority systems & networks									
			In-depth knowledge of DoD security/IA policy, CERT member training reqs., & sources of training for CERT members		Ability to develop an effective incident response/incident handling team							
				Budget mgmt. for CERT operations	Ability to create, defend & manage a budget.							
					Manage conduct of systemic analysis of attack implications							

Function	Certification		Performance Items			Func. Spec.	Demonstration		Sign-Off	Certification		Re- Certification
			[Manage, Acquire, Design & Develop, Implement & Operate, Review & Evaluate, Use, Other]							Validity		
<i>Privileged Access</i>	<i>Pre-Reqs. or Equivalent</i>	<i>Topical Areas or Courses</i>	<i>Knowledge</i>	<i>Skills</i>	<i>Abilities</i>		<i>Test</i>	<i>On-the- Job</i>	<i>Cmd. - Level</i>	<i>Admin.</i>	<i>Other Triggers</i>	<i>Reqs. & Policies</i>
					Manage production of standard & emergency restorral orders, destruction plans, & continuity of operations plans.							
					Advise higher mgmt. on IA & INFOSEC issues & recommend performance & security improvements.							

Appendix K. Service/Agency Costs to Implement Recommendation

Table 43. Service/Agency Costs to Implement Recommendations

Service/ Agency	Cost by Recommendation				Total Cost by Service/Agency
	Recomm. 1 (See Section 2.1.1)	Recomm. 9 (See Section 3.1.1)	Recomm. 14 (See Section 3.3.2)	Recomm. 18 (See Section 3.3.3)	
JCS	No cost		\$25K	No cost	\$25K
Army	\$3M		\$1M	No cost	\$4M
Navy	\$5.5M		\$1.5M	No cost	\$7M
Air Force	\$3M		\$1M	No cost	\$4M
Marine Corps	\$75K		\$0.5M	No cost	\$575K
OSD	DMDC - \$50K CPMS - Unknown		No cost	Year 1 - \$5M Years 2 -5 - \$10M each	\$45.05M
DIA	\$400K		\$750K	Years 1-5:750K each	\$4.9M
NSA	\$500K		\$2.5M	No cost	\$3M
DLA	No cost		\$1.5M	No cost	\$1.5M
WHS	No cost		No cost	No cost	No cost
DISA	No cost		\$720K	No cost	\$720K
NIMA	No cost		\$720K	No cost	\$720K
BMDO	No cost		\$250K	No cost	\$250K
IRMC		\$5.8M			\$5.8M
Total Cost by Recommendation	\$12.525	\$5.8M	\$10.465M	\$48.75M	\$77.5M

Appendix L. Schedule of Recommendations

Task Name Management (continuous)	Year 1				Year 2				Year 3				Year 4				Year 5				Yes	
	M1	M4	M7	M10	M13	M16	M19	M22	M25	M28	M31	M34	M37	M40	M43	M46	M49	M52	M55	M58		M61
Decision to Implement Recommendations																						
Recommendation 1: Database (Y2K)																						
Recommendation 2: Inherently Governmental																						
Recommendation 3: Core IT/IA Mission Capabilities																						
Recommendation 4: Contractor Database																						
Recommendation 5: Staffing Group																						
Recommendation 6: Publicize OPM Recruiting/Retention Plan																						
Recommendation 7: CIO Certificate																						
Recommendation 8: Implement Annual Executive Session																						
Recommendation 9: ISMC Funding & Personnel																						
Recommendation 10: CAPSTONE/APEX																						
Recommendation 11: Glossary																						
Recommendation 12: JMET/JUTL																						
Recommendation 13: Adopt NIST/IC Standards																						
Recommendation 14: Mandatory IA Training/Certification																						
Recommendation 15: Entry Level (privileged access)																						
Recommendation 16: Document Certification Implementation																						
Recommendation 17: DIAP Biennial Certification Reviews																						
Recommendation 18: Advanced Distributed Learning (ADL)																						
Recommendation 19: Promulgate Contractors Directive																						

References

- 1996 Clinger-Cohen Act, Section 5125(C)(3).
- Clinger-Cohen Competencies, revised 25 September 1998.
- Defense Science Board. Report on Information Warfare – Defense. November 1996.
- Department of Commerce, National Institute for Technology and Standards. NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model.
- Department of Defense. DODD 8500.xx, Information Assurance.
- Department of Defense. Joint Vision 2010.
<http://www.dtic.mil/doctrine/jv2010/jvpub.htm>
- Department of Defense. NSTISSC National Training Standard Instructions.
- Department of Defense. NSTISSI Number 4009, National Information Systems Security (INFOSEC) Glossary.
- Department of Defense, Deputy Secretary of Defense. Memorandum: Department of Defense Reform Initiative Directive #27 — DoD Computer Forensics Laboratory and Training Program. 10 February 1998.
- Department of Defense, Deputy Secretary of Defense. Memorandum: Information Vulnerability and the World Wide Web. 24 September 1998.
- General Accounting Office. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. GAO/AIMD-96-84. May 1996.
- Inherently Governmental and Commercial Activities Inventory Report.
- Office of Personnel Management. Recruiting and Retaining Information Technology Professionals. [n.d.]
- Office of the Secretary of Defense. [memorandum: Establishing the IT/IA IPT]. September 22, 1998.
- President of the United States. Executive Order 13111. January 1999.
- NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, and the NSTISSC National Training Standard Instructions.

Acronyms and Abbreviations

.			
A&T	Acquisition and Technology	DoD IG	Department of Defense Inspector General
ADP	Automated Data Processing	DSB	Defense Science Board
AIS	Automated Information Systems	DSS	Defense Security Service
ASD	Assistant Secretary of Defense	E-	enlisted
BMDO	Ballistic Missile Defense Organization	EO	Executive Order
C2	command and control	ESOP	Employee Stock Option Plans
C3I	command, control, communications, and intelligence	FA	Functional Area
C4I	command, control, communications, computers, and intelligence	FT	Fireman Technician
C-E	Communications-Electronics	FY	fiscal year
CBT	computer-based training	GAO	General Accounting Office
CERT	Computer Emergency Response Team	GAR	grade adjusted recapitulation
CF	Career Field	GPRA	Government Performance and Reporting Act
CFO	Chief Financial Officer	GS	General Schedule
CINC	commander in chief	HQ	headquarters
CIO	Chief Information Officer	IA	information assurance
CISN	Computers, Information Systems and Networks	IG	Inspector General
CMF	Career Management Field	IGWG	Inherently Governmental Working Group
COL	colonel	INFOSEC	Information Security
COO	Chief Operations Officer	INTEL	intelligence
CPMS	Civilian Personnel Management Service	IO	Information Operations
CT	Cryptologic Technician	IPT	Integrated Process Team
DAU	Defense Acquisition University	IRMC	Information Resources Management College
DCIO	Deputy Chief Information Officer	ISSM	Information System Security Manager
DEPSECDEF	Deputy Secretary of Defense	ISSO	Information System Security Officer
DFAS	Defense Finance and Accounting Service	IT	information technology
DIA	Defense Intelligence Agency	ITM	information technology management
DIAP	Defense-Wide Information Assurance Program	IW	information warfare
DISA	Defense Information Systems Agency	JMETL	Joint Mission Essential Task List
DLA	Defense Logistics Agency	JS	Joint Staff
DMDC	Defense Manpower Data Center	JV	Joint Vision
DP	Data Processing	LTC	lieutenant colonel
DoD	Department of Defense		
DODD	Department of Defense Directive		

K	thousand	PC	personal computer
M	million	PDD	Presidential Decision Directive
MAJ	major	PERSCOM	Personnel Command
MOS	Military Occupational Specialty	PERSTEMPO	personnel tempo
N/A	not applicable	POM	Program Objective Memorandum
n.d.	no date	ppl	people
NDU	National Defense University	PRA	Primary Review Authority
NEC	Naval Enlisted Classification	Q	quarter
NIMA	National Imaging and Mapping Agency	QOL	Quality of Life
NIST	National Institute of Science and Technology	RM	Radioman
NPS	Naval Postgraduate School	ROTC	Reserve Officer Training Corps
NSA	National Security Agency	SES	Senior Executive Service
NSTISSC	National Security Telecommunications and Information Systems Security Committee	SOW	Statement of Work
NSTISSI	National Security Telecommunications and Information Systems Security Instruction	SRB	Selective Reenlistment Bonuses
O-	officer	TBD	to be determined
OASD (C3I)	Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)	UJTL	Universal Joint Task List
OCS	Officer Candidate School	USD	Under Secretary of Defense
ODASD (CPP)	Office of the Deputy Assistant Secretary of Defense (Civilian Personnel Policy)	Web	World Wide Web
ODASD (MPP)	Office of the Deputy Assistant Secretary of Defense (Military Personnel Policy)	WESTHEM	Western Hemisphere
OJT	on the job training	WHS	Washington Headquarters Service
OPM	Office of Personnel Management		
OPMS	Officer Personnel Management System		
OPTEMP	operating tempo		
OSD	Office of the Secretary of Defense		
OUSD (A&T)	Office of the Under Secretary of Defense (Acquisition & Technology)		
OUSD (P&R)	Office of the Under Secretary of Defense (Personnel & Readiness)		